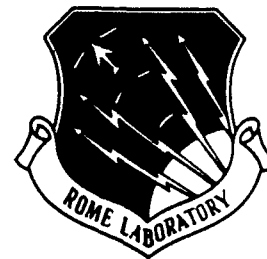


AD-A276 414



RL-TR-93-193
Final Technical Report
October 1993



INTEGRATED TRUSTED SYSTEM DEVELOPMENT ENVIRONMENT-PROCESS

Trusted Information Systems, Inc.

Terry C. Vickers Benzel, Douglas W. Rothnie,
and Stephen D. Crocker

14500 94-07423



DTIC
ELECTE
MAR 07 1994
S E D

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

DTIC QUALITY INSPECTED 1

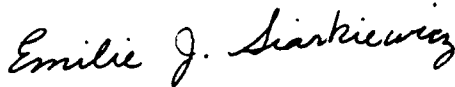
Rome Laboratory
Air Force Materiel Command
Griffiss Air Force Base, New York

94 3 4 055

This report has been reviewed by the Rome Laboratory Public Affairs Office (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

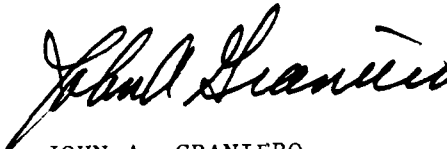
RL-TR-93-193 has been reviewed and is approved for publication.

APPROVED:



EMILIE J. SIARKIEWICZ
Project Engineer

FOR THE COMMANDER:



JOHN A. GRANIERO
Chief Scientist
Command, Control and Communications Directorate

If your address has changed or if you wish to be removed from the Rome Laboratory mailing list, or if the addressee is no longer employed by your organization, please notify RL (C3AB) Griffiss AFB NY 13441. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document require that it be returned.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
<small>Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.</small>				
1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE October 1993	3. REPORT TYPE AND DATES COVERED Final Apr 91 - Dec 92		
4. TITLE AND SUBTITLE INTEGRATED TRUSTED SYSTEM DEVELOPMENT ENVIRONMENT - PROCESS		5. FUNDING NUMBERS C - F30602-91-C-0049 PE - 35167G PR - 1069 TA - 01 WU - P2		
6. AUTHOR(S) Terry C. Vickers Benz, Douglas W. Rothnie, Stephen D. Crocker		8. PERFORMING ORGANIZATION REPORT NUMBER N/A		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Trusted Information Systems, Inc. 11340 Olympic Blvd, Suite 265 Los Angeles CA 90064		9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Rome Laboratory (C3AB) 525 Brooks Rd Griffiss AFB NY 13441-4505		
10. SPONSORING/MONITORING AGENCY REPORT NUMBER RL-TR-93-193		11. SUPPLEMENTARY NOTES Rome Laboratory Project Engineer: Emilie J. Siarkiewicz/C3AB/(315)330-3241		
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited.		12b. DISTRIBUTION CODE -		
13. ABSTRACT (Maximum 200 words) <p>The Integrated Trusted System Development Environment (ITSDE) Process project has further extended and refined the Integrated Development Process (IDP) defined previously by the authors. The result is a set of integrated Data Item Descriptions (DIDs) for use with the process and tailoring directions for producing the DIDs.</p> <p>The IDP describes a software development process for developing trusted systems under DoD-STD-2167A. The process is based on an approach which integrates the Trusted Computer System Criteria (TCSEC) requirements contained in DOD-5200.28-STD into the software development process required by DoD-STD-2167A. The IDP focuses on development of 2167A DIDs which have been tailored to include TCSEC deliverables. The IDP describes how these items can be produced in a manner which minimizes the impact on cost and budget, while increasing assurance in the product's trustworthiness.</p> <p>The majority of the work reported here was performed during the period 1 Apr 91 - 30 May 92. The final contents of this report had been left open during the period 1 Jun 92 - 30 May 93 in anticipation of having the opportunity to update the report to reflect the draft Software Development and Documentation Standard (MIL-STD-SDD), which has been under development and review by the Harmonization Working Group (HWG) of the</p>				
14. SUBJECT TERMS Software Development Process, DoD-STD-2167A, Trusted Systems Development, DoD-5200.28-STD		15. NUMBER OF PAGES 148		
		16. PRICE CODE		
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL	

UNCLASSIFIED

13. ABSTRACT (Continued).

DoD Software Action Plan (SWAP) and the Joint Logistic Commanders Joint Policy Coordinating Group on Computer Resource Management. For many reasons this did not occur. We believe that the information provided here will be of use while the community awaits the new standard; and can serve as a basis for tailoring and adapting the newly developed DIDs for MIL-STD-SDD when they become available.

UNCLASSIFIED

Contents

1	Introduction	2
2	Tailoring Guidance	5
3	Newly Developed DID's	13
4	Intregrated DID's	31
5	Tools	105
6	Conclusion	138
7	References	139

Accession For	
NTIS CRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution /	
Availability Codes	
Dist	Avail and / or Special
A-1	

PREFACE

The majority of the work reported on here was performed during the period April 1, 1991 - May 30, 1992. The final contents of this report have been left open during the period June 1, 1992 - May 30, 1993. It had been anticipated that we would thus have the opportunity to update this report to reflect the draft Software Development and Documentation Standard (MIL-STD-SDD) which has been under development and review by the Harmonization Working Group (HWG) of the Department of Defense Software Action Plan (SWAP) and the Joint Logistics Commanders Joint Policy Coordinating Group on Computer Resource Management. For many reasons this has not occurred. Therefore, we have decided to finalize this report at this time. We believe that the information provided here will be of use while the community awaits the new standard; and can serve as a basis for tailoring and adapting the newly developed DID's for MIL-STD-SDD when they become available.

1 Introduction

The Integrated Trusted System Development Environment, (ITSDE) project has further extended and refined the Integrated Development Process (IDP) defined by [BENZEL]. The result is a set of integrated Data Item Descriptions (DID's) for use with the process and tailoring directions for producing the DID's.

The IDP describes a software development process for developing trusted systems under DoD-STD-2167A. The process is based on an approach which integrates Trusted Computer System Evaluation Criteria (TCSEC) requirements into the software development process required by DoD-STD-2167A. The IDP focuses on development of DoD-STD-2167A Data Item Descriptions which have been tailored to include TCSEC deliverables. The IDP describe how these items can be produced in a manner which minimizes the impact on cost and budget, while increasing assurance in the product's trustworthiness.

The ITSDE project examined the IDP proposed integration strategies in detail. We performed a line by line integration of TCSEC deliverables into existing 2167A DID's. When analyzed in this manner it turned out that some of the integration proposed in the IDP was not in practice feasible. In particular, the IDP suggested that the TCSEC Formal Model and Philosophy of Protection (POP) could be developed during the initial phases of the 2167A development process. Specifically, the IDP suggests that the Philosophy of Protection be developed during the System Requirements Analysis phase and that the 2167A System Segment Specification (SSS) be tailored to include the POP. Further, the IDP suggested that the Formal Security Policy Model be developed during the Software Requirements Analysis phase and that the 2167A Software Requirements Specification (SRS) be tailored to include the formal model. However, results of a parallel effort by ORA and other experiences in the community[FREEMAN] have indicated that this can often be problematic. It now appears that in fact the types of requirements and activities performed during the early 2167A phases and the early TCSEC phases are different in nature.

Both the TCSEC development process and the 2167A development process suffer from incomplete treatment of early concept documents which lay the foundation for requirements specification and design at later stages. The ORA effort suggests that security requirements which form the basis of the formal model are actually first captured as part of pre-contract work. That is, such requirements should be clearly enunciated in the contract RFP and SOW. Others, [BODEAU] have suggested that the 2167A development process needs to include a concept of operations which helps to clarify high level system requirements and principles.

Given these results, we have not included the Formal Security Policy Model and POP in the tailored DID's but rather are providing separate DID's for these two items. In addition to these two newly developed DID's the IDP suggested that new DID's be developed for

assurance correspondences and the covert channel analysis report. Our research led us to conclude that a new DID does not need to be developed for the assurance correspondences. This is particularly true for system targeted at the B3 or lower level of the TCSEC which requires informal correspondences between the DTLs and the TCB. This is a result of our approach to integrating the DTLs and the 2167A SDD document. This integration allows the DTLs - TCB correspondence to be demonstrated as part of the development process prescribed by DOD-STD-2167A. That is, the standard requires decomposition of high level design, detailed design, pseudo code and requirements tracability. These in fact are the techniques used to construct the informal DTLs - TCB correspondence. For the very few systems which are developed to meet the A1 level of the TCSEC, there is a separate DID for the FTLs - Code correspondence included in The Guide for Security-Relevant Acquisitions CDRL and DID Handbook[KELLY].

Before developing new DID's for the formal model, the POP, and covert channel analysis, we first examined the Security Relevant DID's developed by the Air Force (HQ ESC/AFCSC/SR). The Guide for Security-Relevant Acquisitions CDRL and DID Handbook[KELLY], does include a DID for the TCSEC Formal Security Policy Model and Covert Channel Analysis. It does not include a DID for the Philosophy of Protection. We examined the trade-offs in using the existing Formal Security Policy Model DID as opposed to developing a new stand alone DID for the IDP. The Air Force DID's have been available in draft form since 1988, and are being used on some current AF acquisitions. Thus, the benefit of community acceptance could be gained from the use of this DID. On the other hand we felt that some aspects of the DID were not consistent with the approach taken by the IDP and in the end felt that greater benefit could be derived from developing a stand alone DID which was more closely aligned with the philosophy of integration found in the IDP.

1.1 Integrated DID's

In defining the integrated DID's we operated from the basic premise that Trusted Functional Requirements (TFR's) are simply *Requirements*. That is, all TFR's should be inherently addressed as part of the software development process with respect to requirements specification, design, and analysis. This is in fact central to the *Integrated Development Process*. Given this, the actual modifications to the existing 2167A DID's are not extensive. In most cases the modifications require that whenever a requirement is trust related that it should be so indicated in the body of the 2167A document. Taking this approach allows all security requirements to be fully addressed in the course of the 2167A development while at the same time clearly indicating the security relevant aspects of the development. We believe using this approach will result in better designed systems, more secure systems and systems whose security is easier to evaluate.

1.2 Structure of This Report

A detailed integration of the TCSEC required deliverables and the 2167A deliverables is an important step. Deciding how to present this material is also important. In order for these results to be widely applicable they must be easily specified on a contract by the government acquisition authority. In order to help facilitate this we have chosen to present our results in three forms: Tailoring Guidance, Integrated DID's, and Data Item Report Outlines indicating where additional security requirements apply. Section 2 of this report presents the tailoring guidance and an explanation of the rational behind the decisions made. Section 3 of this report presents the newly developed DID's for the POP and Formal Security Policy Model. Section 4 of this report presents the fully integrated DID's with the new requirements indicated in bold face. Section 5 of this report describes a software tool developed by Logicon[LOGICON], which can be used to tailor 2167A process, DID's, and generate CDRL's. We have used this tool to generate a sample contract which would require the use of the integrated DID's. This section includes the output of the tools and the Data Item Report Outlines. Finally, Section 6 presents conclusions and possible future directions.

2 Tailoring Guidance

This section presents instructions for tailoring DoD-STD-2167A Data Item Descriptions to DoD 5200.28.STD. in a manner consistent with the Integrated Development Process defined by [BENZEL]. It should be noted that not all DoD-STD-2167A DID's required tailoring.

Introduction

Each of the following sections refers to the DID for a DoD-STD-2167A document, specifying particular sections of the DID to which the tailoring adds text. Unless noted otherwise, the new text goes at the end of the section.

System Segment Specification (DI-CMAN-80008A)

10.1.5.1

This description shall address trust-related operational concepts, which may be illustrated in the system diagram, if possible.

10.1.5.2.1.1

This subparagraph shall identify the trusted-related aspects, if any, of the described state (e.g. a maintenance state in which access controls are not checked).

10.1.5.3.9

This subparagraph shall specify the relevant level of the TCSEC (and/or NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements) for which the system is being developed, and shall enumerate the design and construction requirements imposed by the TCSEC for that level (e.g. modularity for B2 and higher systems). Additionally, the requirements, if any, for evaluation, certification, or accreditation shall be stated.

10.1.5.9

This paragraph shall describe the approach to satisfying the relevant qualification requirements (such as testing, and verification, as applicable depending on the TCSEC level of the system) that are imposed by the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements.

10.1.6.2

This paragraph shall specify penetration testing as a special test, if penetration testing is applicable for the TCSEC level of the system.

System Segment Design Document (DI-CMAN-80534)

10.1.3.2

This overview shall identify the trust-related aspects of the system's purpose.

10.1.5.4

The summary of purpose of each HWCI and CSCI shall identify the trust-related aspects of the purpose, and whether the HWCI or CSCI has any trust-related functional requirements. This shall be indicated in the architecture diagram, if possible. Segment relationship descriptions shall indicate what effect, if any, trust requirements have on the relationship. Each statement of purpose of system external interface shall state what trusted-related functionality is provided by that interface, if any.

10.1.6.1.1

This subparagraph shall identify each trust-related requirement of the HWCI.

10.1.6.2.1

This subparagraph shall identify each trust-related requirement of the CSCI.

Software Requirements Specification (DI-MCCR-80025A)

10.1.5.1

(Before last sentence):

This description shall indicate whether the interface is related to any trust-related requirements.

10.1.5.8

This paragraph shall identify which of the CSCI's requirements are specified in the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements. Each of these requirements shall be identified by a name and a reference to a section of the appropriate requirements document.

10.1.5.9

This paragraph shall identify the CSCI's design constraints that are derived from the requirements of the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements.

10.1.5.10

(After first sentence):

Among the quality factors specified shall be any relevant quality factors (such as resistance to penetration) that are derived from the requirements of the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements. These quality factors shall be identified as derived from trust requirements.

10.1.5.12

(After first sentence):

This paragraph shall identify the requirements that are trust-related.

10.1.6.1

(After first sentence):

Among the qualification methods specified shall be any relevant qualification methods (such as formal methods of analysis) that are derived from the requirements of the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements. These qualification methods shall be identified as derived from trust requirements.

Interface Requirements Specification (DI-MCCR-80026A)

10.1.5.2

(After first sentence):

This paragraph shall describe any trust-related requirements that are satisfied by the interface.

10.1.5.2.2

This paragraph shall describe any security-critical data elements.

Software Design Document (DI-MCCR-80012A)

10.1.5.1

This overview shall identify and describe the trust-related aspects of the CSCI's role in the system, and of each of the CSCI's CSCI external interfaces. The description shall identify each CSCI external interface that is also a TCB interface.

10.1.5.1.1

This paragraph shall identify the trust-related aspects of the purpose of each CSC and each CSC interface, and shall identify each CSC interface that is also a TCB interface.

10.1.5.2.1

(After first sentence):

including a description of the trust-related aspects of the purpose.

(In item a, after 1st sentence):

Identify the requirements that are trust-related.

(In item b, after 1st sentence):

Identify the data-flow of security-critical data.

(In item c, after 1st sentence):

Identify the derived design requirements that are trust-related. Identify the design constraints (such as modularity for B2 and higher systems) that are derived from requirements of the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements.

10.1.6.1

(Before last sentence):

and shall identify all CSU interfaces that are TCB interfaces, and all data-flow of security-critical data.

10.1.6.1.2

(Before last sentence):

including the trust-related aspects of the CSU's purpose.

10.1.6.1.2.1

(Before last sentence):

This subparagraph shall identify which requirements are trust-related, and which design and implementation constraints (such as modularity for B2 and higher systems) are derived from requirements of the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements.

10.1.6.1.2.2

This detailed design information shall identify and describe any aspects that are relevant to trust-related requirements, including but not limited to: security-critical algorithms (e.g. access mediation), handling of trust-related errors (e.g. authentication failure), protection-critical data structures, data files, or databases, and limitations imposed by trust requirements (e.g. resource usage driven by covert channel concerns).

10.1.7

(After first sentence):

identifying those CSCI global data elements that are protection-critical.

10.1.8

These paragraphs shall identify the security-critical data in the database.

10.1.11

There shall be an appendix which summarizes the detailed top-level specification of the CSCI, by enumerating all the TCB interfaces provided by the CSCI, and cross-references each to the CSU section that describes the interface.

Interface Design Document (DI-MCCR-80027A)

10.1.5.2

This paragraph shall describe any trust-related aspects of the purpose of the interface.

10.1.5.2.1

(In item b. at end):

including an indication of whether the data element is security-critical.

Software Development Plan (DI-MCCR-80030A)

10.2.3.4

This paragraph shall identify the Philosophy of Protection document as containing the Verification Plan required by the TCSEC (if applicable). This paragraph shall also identify the Software Test Plan document, the Software Test Description documents, and the Software Test Plan documents as providing the test documentation required by the TCSEC. For the TCSEC requirements for configuration management documentation, this paragraph shall identify the configuration management section of this Software Development Plan document.

10.2.5.4

including those of the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements.

10.2.6.2.1

Included among these techniques shall be those required by the TCSEC (i.e. penetration testing, covert channel analysis, and verification, as applicable depending on the TCSEC level of the system). The description of these techniques shall indicate that they are required by the TCSEC.

10.2.6.2.3

Included among these design standards shall be standards intended to meet the design requirements of the TCSEC (e.g. modularity for B2 and higher systems). The standards shall be identified as such.

10.2.8.1.2

The personnel described shall include personnel for any relevant TCSEC-required evaluation method (e.g. penetration testing, covert channel analysis, depending on the TCSEC level of the system). These evaluation methods shall be identified as being required by the TCSEC.

10.2.10

Included among these other functions shall be those required by the TCSEC: modeling, formal analysis, verification, covert channel analysis, and penetration testing (depending on the TCSEC level of the system). These techniques shall be identified as being required by the TCSEC.

Computer System Operator's Manual (DI-MCCR-80018A)

10.1.5

This section shall describe the operational and administrative functionality related to security (including cautions about functions and privileges that should be controlled when operating the trusted system), and shall provide any other information required by the TCSEC Trusted Facility Manual requirements for the TCSEC level and/or interpretations.

Software User's Manual (DI-MCCR-80019A)

10.1.5

(After first sentence):

This section shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

3 Newly Developed DID's

This section presents newly developed DID's for the Formal Security Policy Model. Philosophy of Protection, and Covert Channel Analysis.

DATA ITEM DESCRIPTION

FORMAL SECURITY POLICY MODEL

DI-MCCR-xxxxxx-SDE

3. DESCRIPTION/PURPOSE

3.1 The Formal Security Policy Model (FSPM) provides a formal statement of a model of the security policy enforced by a system.

(continued on page 2)

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for a report describing the formal model which is required of systems to which the DOD Trusted Computer System Evaluation Criteria are applied, at the Trusted Computing Base Classes B2, B3, or A1.

7.2 The Contract Data Requirements List should specify whether this document is to be prepared and delivered on bound 8 1/2 by 11 inch bond paper or electronic media. If electronic media is selected, the precise format must be specified.

(continued on page 2)

10. PREPARATION INSTRUCTIONS

10.1 Content and format instructions. Production of this document using automated techniques is encouraged. Specific content and format instructions for this document are identified below.

- a. Response to tailoring instructions. In the event that a paragraph or subparagraph has been tailored out, a statement to that effect shall be added directly following the heading of each such (sub)paragraph. If a paragraph and all of its subparagraphs are tailored out, only the highest level paragraph heading need be included.
- b. Use of alternate presentation styles. Charts, tables, matrices, or other presentation styles are acceptable when the information required by the paragraphs and subparagraphs of this DID can be made more readable.
- c. Page numbering. Each page prior to Section 1 shall be numbered in lower-case roman numerals beginning with page ii for the Table of Contents. Each page starting from Section 1 to the beginning of the appendixes shall be consecutively numbered in arabic numerals. If the document is divided into volumes, each such volume shall restart the page numbering sequence.

(continued on page 2)

DISTRIBUTION STATEMENT A.

Approved for public release: distribution is unlimited.

3. DESCRIPTION/PURPOSE (continued)

3.2 The FSPM is used by the contractor as part of the design of a system, to gain assurance that the system as modeled can enforce the security policy.

3.3 The FSPM enables the government to assess whether the system development meets the DOD Trusted Computer System Evaluation Criteria requirement for a formal model.

7. APPLICATION/INTERRELATIONSHIP (continued)

7.x TBD

10. PREPARATION INSTRUCTIONS (continued)

- d. Document control numbers. For hardcopy formats, this document may be printed on one or both sides of each page (single-sided or double-sided). All printed pages shall contain the document control number and the date of the document centered at the top of the page. Document control numbers shall include revision and volume identification, as applicable.
- e. Multiple (sub)paragraphs. All paragraphs and subparagraphs starting with the phrase "This (sub)paragraph shall..." may be written as multiple subparagraphs to enhance readability. These subparagraphs shall be numbered sequentially.
- f. Document structure. This document shall consist of the following:
 - (1) Cover
 - (2) Title page
 - (3) Table of Contents
 - (4) Scope
 - (5) Referenced Documents
 - (6) Formal Computer Security Policy Model
 - (7) Notes
 - (8) Appendixes.

10.1.1 Title page. The title page shall contain the information identified below in the indicated format:

[Document control number and date: Volume x of y (if multi-volume)]
 [Rev. indicator: date of Rev.]

FORMAL SECURITY POLICY MODEL

FOR THE

[SYSTEM NAME]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

Prepared for:

[Contracting Agency Name, department code]

Prepared by:

[contractor name and address]

Authenticated by _____
 (Contracting agency)

Approved by _____
 (Contractor)

Date _____

Date _____

10.1.2 Table of contents. This document shall contain a table of contents listing the title and page number of each titled paragraph and subparagraph. The table of contents shall then list the title and page number of each figure, table, and appendix, in that order.

10.1.3 Scope. This section shall be numbered 1 and shall be divided into the following paragraphs.

10.1.3.1 Identification. This paragraph shall be numbered 1.1 and shall contain the approved identification number, title, and abbreviation, if applicable, of the system to which this FSPM applies.

10.1.3.2 System overview. This paragraph shall be numbered 1.2 and shall briefly state the purpose of the system to which this FSPM applies.

10.1.3.3 Document overview. This paragraph shall be numbered 1.3 and shall summarize the purpose and contents of this document.

10.1.4 Applicable documents. This section shall be numbered 2 and shall be divided into the following paragraphs.

10.1.4.1 Government documents. This paragraph shall be numbered 2.1. This paragraph shall begin with one of the following two paragraphs, as applicable: (1) "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement." (2) "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement, except for specification (enter number of next higher-tiered specification) listed below." The following paragraph shall appear at the conclusion of the list of documents: "Copies of specifications, standards, drawings, and publications required by suppliers in connection with specified procurement functions should be obtained from the contracting agency or as directed by the contracting officer." Government documents shall be listed by document number and title in the following order:

SPECIFICATIONS:

Federal
Military
Other Government Agency

STANDARDS:

Federal
Military
Other Government Agency

DRAWINGS:

(Where detailed drawings referred to in a specification are listed on an assembly drawing, it is only necessary to list the assembly drawing.)

OTHER PUBLICATIONS:

Manuals
Regulations
Handbooks
Bulletins
etc.

10.1.4.2 Non-Government documents. This paragraph shall be numbered 2.2 and shall begin with the following paragraph: "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement." The source for all documents not available through normal Government stocking activities shall be listed. The following paragraph shall be placed at the conclusion of the list when applicable: "Technical society and technical association specifications and standards are generally available for reference from libraries. They are also distributed among technical groups and using Federal Agencies." Non-Government documents shall be listed by document number and title in the following order:

SPECIFICATIONS:

STANDARDS:

DRAWINGS:

OTHER PUBLICATIONS:

10.1.5 Formal Computer Security Policy Model This section shall be numbered 3 and shall be divided into the following paragraphs to describe the Formal Computer Security Policy Model of the system.

10.1.5.1 Security Policy This paragraph shall be numbered 3.1 and shall state the security policy to be modeled. The security policy statement shall identify the classes of subjects and objects controlled by the TCB, as well as the rules for controlling access to objects by subjects. In addition to an English language description of the policy, this paragraph shall also provide a set of formalized statements of the policy, called policy axioms.

10.1.5.2 Model Development This paragraph shall be numbered 3.2 and shall be divided into the following subparagraphs to describe the development of the model.

10.1.5.2.1 Considered Models This subparagraph shall be numbered 3.2.1 and shall describe, in conceptual terms, the relative advantages and disadvantages of each of the various model types considered for use. Model types may include state transition, temporal logic, denotational semantics, or algebraic specification models.

10.1.5.2.1 Chosen Model This subparagraph shall be numbered 3.2.2 and shall discuss in detail the types of model chosen, and explain why these types were selected over the other considered model types.

10.1.5.3 Background This paragraph shall be numbered 3.3 and shall describe the formal background for the statement of the model. This background material shall describe all assumptions implicit in the model, mathematical axioms upon which the model is founded, theorems used in the statement of the model (along with literature references for the proofs of the theorems), logical notations in which the model is stated, and any other ancillary notation or concept used in the statement of the model. For each element of the background of the model, an English language description shall be provided in addition to a mathematical statement (if any), and an explanation of why the element is necessary to the model, and a description of its relationship to other elements of the model background.

10.1.5.4 Preliminaries This paragraph shall be numbered 3.4 and shall describe the formal preliminaries for the model, including all types and functions used in the statement of the model, and statements of any new theorems used in the statement of the model. Proofs of the new theorems shall be given in an appendix. As applicable, describe the relationship to specific security-enforcement mechanisms of the system of any types, functions, theorems, or other preliminary element.

10.1.5.5 Model Statement This paragraph shall be numbered 3.5 and shall describe the model of the policy enforced by the TCB. Provide a formal mathematical description of the model and each of its components, and also an English language description of the model and each of its components. The English language descriptions shall be placed in close proximity to the mathematical statements they describe. Illustrate the model's components with sketches, diagrams, security state transition tables, or other graphic representations. Annotate these graphics with English language descriptions.

10.1.5.6 Traceability This paragraph shall be numbered 3.6 and shall demonstrate that the model is sufficient to describe the enforcement of the security policy, by tracing each of the security policy statements and policy axioms to a formal statement in the model. A cross-reference matrix chart may be used along with detailed explanatory text tracing model elements to policy axioms, in order to prove the consistency of the model with the policy axioms.

10.1.6 Notes This section shall be numbered 4 and shall contain any general information that aids in understanding this document (e.g., background information, glossary). This section shall contain an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document.

10.1.7 Appendixes Appendixes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.), and the paragraphs within each appendix be numbered as multiples of 10 (e.g., Appendix A, paragraph 10, 10.1, 10.2, 20, 20.1, 20.2, etc.). Pages within each appendix shall be numbered alpha-numerically as follows: Appendix A pages shall be numbered A-1, A-2, A-3, etc. Appendix B pages shall be numbered B-1, B-2, B-3, etc.

10.1.7.1 Mathematical Proofs An appendix shall provide proofs of new theorems, if any, stated in the preliminaries in paragraph 3.4. Each proof shall provide both the mathematical proof and also an English language description of the proof.

DATA ITEM DESCRIPTION

PHILOSOPHY OF PROTECTION

DI-MCCR-xxxxx-SDE

3. DESCRIPTION/PURPOSE

3.1 The Philosophy of Protection (PoP) describes the essential concepts, the security policy, and the protection mechanisms of the Trusted Computing Base (TCB) of a system.

(continued on page 2)

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for a report containing the protection mechanism description which must be provided for systems to which the DOD Trusted Computer System Evaluation Criteria are applied.

7.2 The Contract Data Requirements List should specify whether this document is to be prepared and delivered on bound 8 1/2 by 11 inch bond paper or electronic media. If electronic media is selected, the precise format must be specified.

(continued on page 2)

10. PREPARATION INSTRUCTIONS

10.1 Content and format instructions. Production of this document using automated techniques is encouraged. Specific content and format instructions for this document are identified below.

- a. Response to tailoring instructions. In the event that a paragraph or subparagraph has been tailored out, a statement to that effect shall be added directly following the heading of each such (sub)paragraph. If a paragraph and all of its subparagraphs are tailored out, only the highest level paragraph heading need be included.
- b. Use of alternate presentation styles. Charts, tables, matrices, or other presentation styles are acceptable when the information required by the paragraphs and subparagraphs of this DID can be made more readable.
- c. Page numbering. Each page prior to Section 1 shall be numbered in lower-case roman numerals beginning with page ii for the Table of Contents. Each page starting from Section 1 to the beginning of the appendixes shall be consecutively numbered in arabic numerals. If the document is divided into volumes, each such volume shall restart the page numbering sequence.

(continued on page 2)

DISTRIBUTION STATEMENT A.

Approved for public release; distribution is unlimited.

3. DESCRIPTION/PURPOSE (continued)

3.2 The PoP is used by the contractor as part of the development of a system, to ensure that all essential security concepts and TCB features are well understood and explicitly documented.

3.3 The PoP enables the government to assess whether the system's security-related functionality is clearly articulated and is appropriate for a system which must meet the requirements of the DOD Trusted Computer System Evaluation Criteria.

7. APPLICATION/INTERRELATIONSHIP (continued)

7.x TBD

10. PREPARATION INSTRUCTIONS (continued)

- d. Document control numbers. For hardcopy formats, this document may be printed on one or both sides of each page (single-sided or double-sided). All printed pages shall contain the document control number and the date of the document centered at the top of the page. Document control numbers shall include revision and volume identification, as applicable.
- e. Multiple (sub)paragraphs. All paragraphs and subparagraphs starting with the phrase "This (sub)paragraph shall..." may be written as multiple subparagraphs to enhance readability. These subparagraphs shall be numbered sequentially.
- f. Document structure. This document shall consist of the following:
 - (1) Cover
 - (2) Title page
 - (3) Table of Contents
 - (4) Scope
 - (5) Referenced Documents
 - (6) Philosophy of Protection
 - (7) Notes
 - (8) Appendixes.

10.1.1 Title page. The title page shall contain the information identified below in the indicated format:

[Document control number and date: Volume x of y (if multi-volume)]
 [Rev. indicator: date of Rev.]

PHILOSOPHY OF PROTECTION

FOR THE

[SYSTEM NAME]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

Prepared for:

[Contracting Agency Name, department code]

Prepared by:

[contractor name and address]

Authenticated by _____
 (Contracting agency)

Date _____

Approved by _____
 (Contractor)

Date _____

10.1.2 Table of contents. This document shall contain a table of contents listing the title and page number of each titled paragraph and subparagraph. The table of contents shall then list the title and page number of each figure, table, and appendix, in that order.

10.1.3 Scope. This section shall be numbered 1 and shall be divided into the following paragraphs.

10.1.3.1 Identification. This paragraph shall be numbered 1.1 and shall contain the approved identification number, title, and abbreviation, if applicable, of the system to which this POP applies.

10.1.3.2 System overview. This paragraph shall be numbered 1.2 and shall briefly state the purpose of the system to which this POP applies.

10.1.3.3 Document overview. This paragraph shall be numbered 1.3 and shall summarize the purpose and contents of this document.

10.1.4 Applicable documents. This section shall be numbered 2 and shall be divided into the following paragraphs.

10.1.4.1 Government documents. This paragraph shall be numbered 2.1. This paragraph shall begin with one of the following two paragraphs, as applicable: (1) "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement." (2) "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement, except for specification (enter number of next higher-tiered specification) listed below." The following paragraph shall appear at the conclusion of the list of documents: "Copies of specifications, standards, drawings, and publications required by suppliers in connection with specified procurement functions should be obtained from the contracting agency or as directed by the contracting officer." Government documents shall be listed by document number and title in the following order:

SPECIFICATIONS:

- Federal
- Military
- Other Government Agency

STANDARDS:

- Federal
- Military
- Other Government Agency

DRAWINGS:

(Where detailed drawings referred to in a specification are listed on an assembly drawing, it is only necessary to list the assembly drawing.)

OTHER PUBLICATIONS:

- Manuals
- Regulations
- Handbooks
- Bulletins
- etc.

10.1.4.2 Non-Government documents. This paragraph shall be numbered 2.2 and shall begin with the following paragraph: "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement." The source for all documents not available through normal Government stocking activities shall be listed. The following paragraph shall be placed at the conclusion of the list when applicable: "Technical society and technical association specifications and standards are generally available for reference from libraries. They are also distributed among technical groups and using Federal Agencies." Non-Government documents shall be listed by document number and title in the following order:

SPECIFICATIONS:

STANDARDS:

DRAWINGS:

OTHER PUBLICATIONS:

10.1.5 Philosophy of Protection This section shall be numbered 3 and shall be divided into the following paragraphs to describe the contractor's philosophy of protection and to explain how this philosophy is applied to the system's Trusted Computing Base (TCB).

10.1.5.1 Security Objects and Subjects This section shall be numbered 3.1 and shall explicitly identify and define the classes of security objects and subjects provided by the TCB. Describe what actual operational resources (such as users, programs, files, devices, and the like) the TCB uses to provide these objects and subjects, and in particular, describe how subjects are related to users. Note which actual operational resources, if any, are not controlled by the TCB. Note which actual operational resources, if any, are controlled by the TCB but are not made directly available as a subject or object. Distinguish between those security objects which are named, and those that are not.

10.1.5.2 Security Policy and Access Controls This section shall be numbered 3.2 and shall describe the security policy enforced by the TCB of the system, including policies about the interactions of security objects and subjects. Other aspects of the policy may include (but are not limited to) access controls, identification and authentication, trusted path, auditing, integrity, and availability. Discussion of access controls shall state all the rules which permit and constrain how subjects are allowed access to objects. Discretionary Access Control and Mandatory Access Control (applicable only for systems intended to meet TCSEC class B or A requirements) shall be discussed separately from one another.

10.1.5.3 TCB Protection Mechanisms This section shall be numbered 3.3 and shall identify the specific protection mechanisms used by the TCB to enforce the system's security policy. For each mechanism, its role in policy shall be described, as well as its relationship to other mechanisms. Note which protection mechanisms are, or directly rely upon, hardware features, and identify all of the TCB's uses of hardware features. Identify those protection mechanisms which the TCB uses to protect itself, and explain their role in doing so. Identify those protection mechanisms that used to enforce access controls, and explain their role in doing so. Identify all instances in which access control mechanisms are also used for TCB protection (e.g. storing TCB data in a storage object controlled by DAC).

10.1.5.4 Reference Monitor This section shall be numbered 3.4 and shall describe how the system's TCB implements the reference monitor concept, including an explanation why it is tamper resistant, cannot be bypassed, and is correctly implemented. This section applies only to systems intended to meet the requirements of the TCSEC levels B2, B3, and A1.

10.1.5.5 Privilege This section shall be numbered 3.5 and shall describe all privileged conditions under which any subjects are exempted from the operational restrictions of the system's TCB. Identify all privileges which permit a subject to be exempt from the enforcement of any aspect of the security policy, including (but not limited to) exemptions from the enforcement of access control rules. Describe the manner in which privileges are assigned to subjects, and describe the controls enforced on these assignments. Explain the role of protection mechanisms in the enforcement of these controls.

10.1.5.6 Trusted Subjects This section shall be numbered 3.6 and shall describe all subjects which may be assigned any privilege which may permit exemptions from the enforcement of any aspect of the security policy. Each description shall include a brief summary of the purposes and roles of the trusted subject, the relevant privileges it may be assigned, the use it makes of the privilege, and an explanation of how the trusted subject may relate to a user or users.

10.1.5.7 Verification Plan This section shall be numbered 3.7 and shall describe the technical approach to carrying out the formal specification and verification of the systems. This section is applicable only for systems intended to meet the A1 level of the TCSEC. For each of the following, this section shall describe the formal specification and verification approach used to satisfy the formal specification and verification requirements of the TCSEC:

- a. Formal Security Policy Model
- b. Formal Top-Level Specification
- c. Descriptive Top-Level Specification
- d. Code Correspondence
- e. Covert Channel Analysis

10.1.6 Notes This section shall be numbered 4 and shall contain any general information that aids in understanding this document (e.g., background information, glossary). This section shall contain an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document.

10.1.7 Appendixes Appendixes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.), and the paragraphs within each appendix be numbered as multiples of 10 (e.g., Appendix A, paragraph 10, 10.1, 10.2, 20, 20.1, 20.2, etc.). Pages within each appendix shall be numbered alpha-numerically as follows: Appendix A pages shall be numbered A-1, A-2, A-3, etc. Appendix B pages shall be numbered B-1, B-2, B-3, etc.

DATA ITEM DESCRIPTION

COVERT CHANNEL ANALYSIS

DI-MCCR-xxxxx-SDE

3. DESCRIPTION/PURPOSE

3.1 This DID specifies the content and format of a Technical Report that documents covert channel analyses (CCA) for a system.

(continued on page 2)

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for a report describing the covert channel analysis which is required of systems to which the DOD Trusted Computer System Evaluation Criteria are applied, at the Trusted Computing Base Classes B2, B3, or A1.

7.2 The Contract Data Requirements List should specify whether this document is to be prepared and delivered on bound 8 1/2 by 11 inch bond paper or electronic media. If electronic media is selected, the precise format must be specified.

(continued on page 2)

10. PREPARATION INSTRUCTIONS

10.1 Content and format instructions. Production of this document using automated techniques is encouraged. Specific content and format instructions for this document are identified below.

- a. Response to tailoring instructions. In the event that a paragraph or subparagraph has been tailored out, a statement to that effect shall be added directly following the heading of each such (sub)paragraph. If a paragraph and all of its subparagraphs are tailored out, only the highest level paragraph heading need be included.
- b. Use of alternate presentation styles. Charts, tables, matrices, or other presentation styles are acceptable when the information required by the paragraphs and subparagraphs of this DID can be made more readable.
- c. Page numbering. Each page prior to Section 1 shall be numbered in lower-case roman numerals beginning with page ii for the Table of Contents. Each page starting from Section 1 to the beginning of the appendixes shall be consecutively numbered in arabic numerals. If the document is divided into volumes, each such volume shall restart the page numbering sequence.

(continued on page 2)

DISTRIBUTION STATEMENT A.

Approved for public release; distribution is unlimited.

3. DESCRIPTION/PURPOSE (continued)

3.2 The CCA is performed by the contractor as part of the design and implementation of a system, to gain assurance that the system as designed and implemented will enforce the security policy. In general, CCA has 3 distinct components: 1) identification of covert channels, 2) estimation of their capacities, and 3) reduction of capacities.

3.3 The CCA enables the government to assess whether the system development meets the DOD Trusted Computer System Evaluation Criteria requirement for CCA.

7. APPLICATION/INTERRELATIONSHIP (continued)

7.x TBD

10. PREPARATION INSTRUCTIONS (continued)

- d. Document control numbers. For hardcopy formats, this document may be printed on one or both sides of each page (single-sided or double-sided). All printed pages shall contain the document control number and the date of the document centered at the top of the page. Document control numbers shall include revision and volume identification, as applicable.
- e. Multiple (sub)paragraphs. All paragraphs and subparagraphs starting with the phrase "This (sub)paragraph shall..." may be written as multiple subparagraphs to enhance readability. These subparagraphs shall be numbered sequentially.
- f. Document structure. This document shall consist of the following:
 - (1) Cover
 - (2) Title page
 - (3) Table of Contents
 - (4) Scope
 - (5) Referenced Documents
 - (6) Covert Channel Analysis
 - (7) Notes
 - (8) Appendixes.

10.1.1 Title page. The title page shall contain the information identified below in the indicated format:

[Document control number and date: Volume x of y (if multi-volume)]
 [Rev. indicator: date of Rev.]

COVERT CHANNEL ANALYSIS

FOR THE

[SYSTEM NAME]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

Prepared for:

[Contracting Agency Name, department code]

Prepared by:

[contractor name and address]

Authenticated by _____
 (Contracting agency)

Approved by _____
 (Contractor)

Date _____

Date _____

10.1.2 Table of contents. This document shall contain a table of contents listing the title and page number of each titled paragraph and subparagraph. The table of contents shall then list the title and page number of each figure, table, and appendix, in that order.

10.1.3 Scope. This section shall be numbered 1 and shall be divided into the following paragraphs.

10.1.3.1 Identification. This paragraph shall be numbered 1.1 and shall contain the approved identification number, title, and abbreviation, if applicable, of the system to which this CCA applies.

10.1.3.2 System overview. This paragraph shall be numbered 1.2 and shall briefly state the purpose of the system to which this CCA applies.

10.1.3.3 Document overview. This paragraph shall be numbered 1.3 and shall summarize the purpose and contents of this document.

10.1.4 Applicable documents. This section shall be numbered 2 and shall be divided into the following paragraphs.

10.1.4.1 Government documents. This paragraph shall be numbered 2.1. This paragraph shall begin with one of the following two paragraphs, as applicable: (1) "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement." (2) "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement, except for specification (enter number of next higher-tiered specification) listed below." The following paragraph shall appear at the conclusion of the list of documents: "Copies of specifications, standards, drawings, and publications required by suppliers in connection with specified procurement functions should be obtained from the contracting agency or as directed by the contracting officer." Government documents shall be listed by document number and title in the following order:

SPECIFICATIONS:

Federal
Military
Other Government Agency

STANDARDS:

Federal
Military
Other Government Agency

DRAWINGS:

(Where detailed drawings referred to in a specification are listed on an assembly drawing, it is only necessary to list the assembly drawing.)

OTHER PUBLICATIONS:

Manuals
Regulations
Handbooks
Bulletins
etc.

10.1.4.2 Non-Government documents. This paragraph shall be numbered 2.2 and shall begin with the following paragraph: "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement." The source for all documents not available through normal Government stocking activities shall be listed. The following paragraph shall be placed at the conclusion of the list when applicable: "Technical society and technical association specifications and standards are generally available for reference from libraries. They are also distributed among technical groups and using Federal Agencies." Non-Government documents shall be listed by document number and title in the following order:

SPECIFICATIONS:

STANDARDS:

DRAWINGS:

OTHER PUBLICATIONS:

10.1.5 Covert Channel Analysis This section shall be numbered 3 and shall be divided into the following paragraphs to describe the Covert Channel Analysis of the system.

10.1.5.1 Methodology This paragraph shall be numbered 3.1 and shall state the methodologies used for:

- Identification
- Bandwidth Estimation
- Reduction of Bandwidth

10.1.5.2 Description of Channels This paragraph shall be numbered 3.2 and shall be divided into the following subparagraphs to describe the covert channels identified. The description shall be in English prose and shall describe each of the channels identified and the corresponding exploitation scenarios.

10.1.5.2.1 Storage Channels This subparagraph shall be numbered 3.2.1 and shall describe the channels for which the transmission of information involves the alteration and observation of storage locations in the Trusted Computing Base of the system.

10.1.5.2.1 Timing Channels This subparagraph shall be numbered 3.2.2 and shall describe the channels for which the transmission of information involves the manipulation by the sender of the length of time that the receiver requires to perform some operation.

10.1.5.3 Bandwidths This paragraph shall be numbered 3.3 and shall describe estimated *Worst Case* bandwidths of each of the identified channels. Bandwidth estimates can be obtained through analytical means, engineering estimates, or by actual exercising of the channel and direct measurement. For each channel the bandwidth calculation method used shall be identified.

10.1.5.4 Reduction of Bandwidth This paragraph shall be numbered 3.4 and shall describe the reduction in bandwidth achieved for each channel and how that reduction was achieved.

10.1.5.5 Summary Table This paragraph shall be numbered 3.5 and shall provide a summary table which identifies each channel, its estimated worst case bandwidth and its estimated bandwidth after reduction techniques are applied. The table shall also indicate whether the channel is audited by the system.

10.1.6 Notes This section shall be numbered 4 and shall contain any general information that aids in understanding this document (e.g., background information, glossary). This section shall contain an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document.

10.1.7 Appendixes Appendixes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.), and the paragraphs within each appendix be numbered as multiples of 10 (e.g., Appendix A, paragraph 10, 10.1, 10.2, 20, 20.1, 20.2, etc.). Pages within each appendix shall be numbered alpha-numerically as follows: Appendix A pages shall be numbered A-1, A-2, A-3, etc. Appendix B pages shall be numbered B-1, B-2, B-3, etc.

4 Integrated DID's

This section presents the fully integrated Data Item Descriptions. That is, the following DID's are the result of applying the tailoring guidance described in Section 2 to the DoD-STD-2167A DID's. These DID's were developed using the \LaTeX document preparation system. A tape containing the source code for these DID's has been provided with this final report.

DATA ITEM DESCRIPTION

SYSTEM/SEGMENT SPECIFICATION

DI-CMAN-80008A-SDE

3. DESCRIPTION/PURPOSE

3.1 The System/Segment Specification (SSS) specifies the requirements for a system or a segment of a system. Upon Government approval and authentication, the SSS becomes the Functional Baseline for the system or segment.

(continued on page 2)

880229

AF-10

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for data generated under the work tasks described by paragraph 3.1.3.1 of MIL-STD-490.

7.2 The Contract Data Requirements List should specify whether this document is to be prepared and delivered on bound 8 1/2 by 11 inch bond paper or electronic media. If electronic media is selected, the precise format must be specified.

(continued on page 2)

F4328

10. PREPARATION INSTRUCTIONS

10.1 Content and format instructions. Production of this specification using automated techniques is encouraged. Specific content and format instructions for this specification are identified below.

- a. Response to tailoring instructions. In the event that a paragraph or subparagraph has been tailored out, a statement to that effect shall be added directly following the heading of each such (sub)paragraph. If a paragraph and all of its subparagraphs are tailored out, only the highest level paragraph heading need be included.
- b. Use of alternate presentation styles. Charts, tables, matrices, or other presentation styles are acceptable when the information required by the paragraphs and subparagraphs of this DID can be made more readable.
- c. Page numbering. Each page prior to Section 1 shall be numbered in lower-case roman numerals beginning with page ii for the Table of Contents. Each page starting from Section 1 to the beginning of the appendixes shall be consecutively numbered in arabic numerals. If the document is divided into volumes, each such volume shall restart the page numbering sequence.

(continued on page 2)

DISTRIBUTION STATEMENT A.

Approved for public release; distribution is unlimited.

3. DESCRIPTION/PURPOSE (continued)

3.2 The SSS provides a general overview of the system or segment that may be used by training personnel, support personnel, or users of the system.

7. APPLICATION/INTERRELATIONSHIP (continued)

7.3 The word "system" is used generically in this DID to mean either a system or a segment, as applicable.

7.4 System division into segments normally occurs if parts of the system are:

- a. Assigned to different contractors or government organizations
- b. Intended to be added in an evolutionary or incremental manner
- c. Planned for major modification.

7.5 This DID supersedes DI-CMAN-80008 dated 4 June 1985.

10. PREPARATION INSTRUCTIONS (continued)

- d. Document control numbers. For hardcopy formats, this document may be printed on one or both sides of each page (single-sided or double-sided). All printed pages shall contain the document control number and the date of the document centered at the top of the page. Document control numbers shall include revision and volume identification, as applicable.
- e. Multiple (sub)paragraphs. All paragraphs and subparagraphs starting with the phrase "This (sub)paragraph shall..." may be written as multiple subparagraphs to enhance readability. These subparagraphs shall be numbered sequentially.
- f. Identifiers. The letters "X", "Y", and "Z" serve as identifiers for a series of descriptions. For example, the subparagraphs of 10.1.5.2.1.1 shall be structured as follows:

3.2.1.1 (First system state name)

3.2.1.1.1 (System mode I)

3.2.1.1.1.1 (System capability A)

3.2.1.1.1.2 (System capability B)

3.2.1.1.1.3 (System capability C)

3.2.1.1.2 (System mode J)

3.2.1.1.2.1 (System capability W)

3.2.1.1.2.2 (System capability X)

etc.

3.2.1.2 (Second system state name)

etc.

g. Document structure. This specification shall consist of the following:

- (1) Cover
- (2) Title page
- (3) Table of contents
- (4) Scope
- (5) Applicable documents
- (6) System requirements
- (7) Quality assurance provisions
- (8) Preparation for delivery
- (9) Notes
- (10) Appendixes.

10.1.1 Title page. The title page shall contain the information identified below in the indicated format:

[Document control number and date: Volume x of y (if multi-volume)]
 [Rev. indicator: date of Rev.]

SYSTEM SPECIFICATION
 (OR SEGMENT SPECIFICATION)

FOR THE

[SYSTEM NAME]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

Prepared for:

[Contracting Agency Name, department code]

Prepared by:

[contractor name and address]

Authenticated by _____
 (Contracting agency)

Date _____

Approved by _____
 (Contractor)

Date _____

10.1.2 Table of contents. This specification shall contain a table of contents listing the title and page number of each titled paragraph and subparagraph. The table of contents shall then list the title and page number of each figure, table, and appendix, in that order.

10.1.3 Scope. This section shall be numbered 1 and shall be divided into the following paragraphs.

10.1.3.1 Identification. This paragraph shall be numbered 1.1 and shall contain the approved identification number, title, and abbreviation, if applicable, of the system to which this SSS applies.

10.1.3.2 System overview. This paragraph shall be numbered 1.2 and shall briefly state the purpose of the system to which this SSS applies.

10.1.3.3 Document overview. This paragraph shall be numbered 1.3 and shall summarize the purpose and contents of this document.

10.1.4 Applicable documents. This section shall be numbered 2 and shall be divided into the following paragraphs.

10.1.4.1 Government documents. This paragraph shall be numbered 2.1. This paragraph shall begin with one of the following two paragraphs, as applicable: (1) "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement." (2) "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement, except for specification (enter number of next higher-tiered specification) listed below." The following paragraph shall appear at the conclusion of the list of documents: "Copies of specifications, standards, drawings, and publications required by suppliers in connection with specified procurement functions should be obtained from the contracting agency or as directed by the contracting officer." Government documents shall be listed by document number and title in the following order:

SPECIFICATIONS:

- Federal
- Military
- Other Government Agency

STANDARDS:

- Federal
- Military
- Other Government Agency

DRAWINGS:

(Where detailed drawings referred to in a specification are listed on an assembly drawing, it is only necessary to list the assembly drawing.)

OTHER PUBLICATIONS:

Manuals
Regulations
Handbooks
Bulletins
etc.

10.1.4.2 Non-Government documents. This paragraph shall be numbered 2.2 and shall begin with the following paragraph: "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement." The source for all documents not available through normal Government stocking activities shall be listed. The following paragraph shall be placed at the conclusion of the list when applicable: "Technical society and technical association specifications and standards are generally available for reference from libraries. They are also distributed among technical groups and using Federal Agencies." Non-Government documents shall be listed by document number and title in the following order:

SPECIFICATIONS:

STANDARDS:

DRAWINGS:

OTHER PUBLICATIONS:

10.1.5 System requirements. This section shall be numbered 3 and shall be divided into the following paragraphs and subparagraphs to specify the requirements for the system to which this specification applies.

10.1.5.1 Definition. This paragraph shall be numbered 3.1 and shall provide a brief description of the system. This description shall address pertinent operational, and logistical considerations and concepts. A system diagram shall be provided. *This description shall address trust-related operational concepts, which may be illustrated in the system diagram, if possible.*

10.1.5.2 Characteristics. This paragraph shall be numbered 3.2 and shall be divided into the following subparagraphs to describe the requirements for system performance and physical characteristics.

10.1.5.2.1 Performance characteristics. This subparagraph shall be numbered 3.2.1 and shall be divided into the following subparagraphs to specify the system's capabilities in the context of the states in which the system can exist and the modes of operation within each state. Each capability of the system shall be specified in a uniquely identified subparagraph in order to provide for objective qualification.

10.1.5.2.1.1 (State name). This subparagraph shall be numbered 3.2.1.X (beginning with 3.2.1.1) and shall identify and provide a brief description of a state in which the system can exist (e.g., weapon idle, weapon ready, weapon deployed). *This subparagraph shall identify the trust-related aspects, if any, of the described state (e.g. a maintenance state in which access controls are not checked).*

10.1.5.2.1.1.1 (Mode name). This subparagraph shall be numbered 3.2.1.X.Y (beginning with 3.2.1.1.1). This subparagraph shall identify and provide a brief description of a mode of operation (e.g., surveillance, threat evaluation, weapon assignment, target designation and acquisition, fire control resolution) within the system state identified above.

10.1.5.2.1.1.1.1 (System capability name and project unique identifier). This subparagraph shall be numbered 3.2.1.X.Y.Z (beginning with 3.2.1.1.1.1), shall specify a capability of the system by name and project unique identifier, and shall describe its purpose. This subparagraph shall also identify the applicable parameters associated with the capability and shall express them in measurable terms. If a capability of a mode has been previously defined, this subparagraph shall reference rather than duplicate that information.

10.1.5.2.2 System capability relationships. This subparagraph shall be numbered 3.2.2 and shall summarize the relationships between system capabilities and the states and modes of the system.

10.1.5.2.3 External interface requirements. This paragraph shall be numbered 3.2.3 and shall be divided into the following subparagraphs to describe requirements for interfaces with other systems. Detailed quantitative interface requirements may be defined in separate specifications or Interface Control Documents (ICDs) and referenced herein. All referenced ICDs are considered part of this specification.

10.1.5.2.3.1 (System name) external interface description. This subparagraph shall be numbered 3.2.3.X (beginning with 3.2.3.1) and shall identify an external system with which this system interfaces. This subparagraph shall describe the interfaces to the external system. This subparagraph shall identify the purpose of each interface and shall describe the relationship between each interface and the states and modes of the system. When possible, each interface shall be specified in detailed, quantitative terms (e.g., dimensions, tolerances, loads, speeds, communications protocol).

10.1.5.2.4 Physical characteristics. This subparagraph shall be numbered 3.2.4 and shall specify the requirements for the physical characteristics (e.g., weight limits, dimensional limits) of the system. Additional considerations for determining physical requirements include:

- a. Transportation and storage
- b. Security
- c. Durability
- d. Safety
- e. Vulnerability
- f. Color

10.1.5.2.4.1 Protective coatings. This subparagraph shall be numbered 3.2.4.1 and shall specify, if applicable, protective coating requirements to assure protection from corrosion, abrasion, or other deleterious action.

10.1.5.2.5 System quality factors. This paragraph shall be numbered 3.2.5 and shall be divided into the following subparagraphs to specify the applicable requirements pertaining to system quality factors.

10.1.5.2.5.1 Reliability. This subparagraph shall be numbered 3.2.5.1, shall specify reliability requirements in quantitative terms, and shall define the conditions under which the reliability requirements are to be met. This subparagraph may include a reliability apportionment model to support apportionment of reliability values assigned to system capabilities for their share in achieving desired system reliability.

10.1.5.2.5.2 Maintainability. This subparagraph shall be numbered 3.2.5.2 and shall specify quantitative maintainability requirements. The requirements shall apply to maintenance in the planned maintenance and support environment and shall be stated in quantitative terms. Examples are:

- a. Mean and maximum down time, reaction time, turnaround time, mean and maximum times to repair, mean time between maintenance actions.
- b. Maximum effort required to locate and fix an error.
- c. Maintenance man-hours per flying hour, maintenance man-hours per specific maintenance action, operational ready rate, maintenance hours per operating hour, frequency of preventative maintenance.
- d. Number of people and skill levels, variety of support equipment.
- e. Maintenance costs per operating hour, man-hours per overhaul.

10.1.5.2.5.3 Availability. This subparagraph shall be numbered 3.2.5.3 and shall specify the degree to which the system shall be in an operable and committable state at the start of the mission(s), where the mission(s) is called for at an unknown (random) point in time.

10.1.5.2.5.4 Additional quality factors. This subparagraph shall be numbered 3.2.5.4 and shall specify system quality requirements not defined in the above subparagraphs (e.g., integrity, efficiency, or correctness requirements of the system).

10.1.5.2.6 Environmental conditions. This paragraph shall be numbered 3.2.6 and shall specify the environmental conditions that the system must withstand during transportation, storage, and operation, such as:

- a. Natural environment (e.g., wind, rain, temperature, geographic location)
- b. Induced environment (e.g., motion, shock, noise, electromagnetic radiation)
- c. Environments due to enemy action (e.g., over-pressure, explosions, radiation).

10.1.5.2.7 Transportability. This subparagraph shall be numbered 3.2.7 and shall specify any special requirements for transportation and materials handling. In addition, all system elements that, due to operational or functional characteristics, will be unsuitable for normal transportation methods shall be identified.

10.1.5.2.8 Flexibility and expansion. This subparagraph shall be numbered 3.2.8 and shall specify areas of growth which require planning for system flexibility and expansion. In addition, this subparagraph shall specify specific system elements which require spare capacity to support flexibility and expansion.

10.1.5.2.9 Portability. This subparagraph shall be numbered 3.2.9 and shall specify requirements for portability which are applicable to the system to permit employment, deployment, and logistic support.

10.1.5.3 Design and construction. This paragraph shall be numbered 3.3 and shall be divided into subparagraphs that specify minimum system design and construction standards which have general applicability to system equipment and are applicable to major classes of equipment (e.g., aerospace vehicle equipment, and support equipment) or are applicable to particular design standards. To the maximum extent possible, these requirements shall be specified by incorporation of the established military standards and specifications. Requirements which add to, but do not conflict with, requirements specified herein may be included in individual configuration item specifications. In addition, this paragraph shall specify criteria for the selection and imposition of Federal, military, and contractor specifications and standards.

10.1.5.3.1 Materials. This subparagraph shall be numbered 3.3.1 and shall specify those system-peculiar requirements governing use of materials, parts, and processes in the design of system equipment. Special attention shall be directed to prevent unnecessary use of strategic or critical materials. (A strategic and

critical materials list may be obtained from the contracting agency.) In addition, requirements for the use of standard and commercial parts and parts for which qualified products lists have been established shall be specified in this paragraph.

10.1.5.3.1.1 Toxic products and formulations. This subparagraph shall be numbered 3.3.1.1 and shall specify requirements for the control of toxic products or formulations to be used in the system or to be generated by the system.

10.1.5.3.2 Electromagnetic radiation. This subparagraph shall be numbered 3.3.2 and shall contain requirements pertaining to limits on the electromagnetic radiation which the system is permitted to generate.

10.1.5.3.3 Nameplates and product marking. This subparagraph shall be numbered 3.3.3 and shall contain requirements for nameplates, part marking, serial and lot number marking, software media marking, and other identifying markings required for the system. Reference may be made to existing standards on the content and application of markings.

10.1.5.3.4 Workmanship. This subparagraph shall be numbered 3.3.4 and shall specify workmanship requirements for equipment to be produced during system development and requirements for manufacture by production techniques.

10.1.5.3.5 Interchangeability. This subparagraph shall be numbered 3.3.5 and shall specify the requirements for system equipment to be interchangeable and replaceable. Entries in this paragraph are for the purpose of establishing a condition for design and are not to define the conditions of interchangeability required by the assignment of a part number.

10.1.5.3.6 Safety. This subparagraph shall be numbered 3.3.6 and shall specify those safety requirements which are basic to the design of the system, with respect to equipment characteristics, methods of operation, and environmental influences. This paragraph shall also specify those safety requirements which prevent personnel injury and equipment degradation without degrading operational capability (e.g., restricting the use of dangerous materials where possible, classifying explosives for purposes of shipping, handling and storing, abort/escape provisions from enclosures, gas detection and warning devices, grounding of electrical system, cleanliness and decontamination, explosion proofing).

10.1.5.3.7 Human engineering. This subparagraph shall be numbered 3.3.7 and shall specify human engineering requirements for the system or for specific configuration items. This paragraph shall reference applicable documents (e.g., MIL-STD-1472) and specify any special or unique requirements (e.g., constraints on allocation of capabilities to personnel and communications, and personnel/equipment interactions). This paragraph shall include those specific areas, stations, or equipment which would require concentrated human engineering attention due to the sensitivity of the operation or criticality of the task; i.e., those areas where the effects of human error would be particularly serious.

10.1.5.3.8 Nuclear control. This subparagraph shall be numbered 3.3.8 and shall specify system requirements for nuclear components, such as:

- a. Component design
- b. In-flight control
- c. Prevention of inadvertent detonation
- d. Nuclear safety rules.

10.1.5.3.9 System security. This subparagraph shall be numbered 3.3.9 and shall specify security requirements that are basic to the design of the system with respect to the operational environment of the system. This subparagraph shall also specify those security requirements necessary to prevent compromise of sensitive information or materials. *This subparagraph shall specify the relevant level of the TCSEC (and/or NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements) for which the system is being developed, and shall enumerate the design and construction requirements imposed by the TCSEC for that level (e.g. modularity for B2 and higher systems). Additionally, the requirements, if any, for evaluation, certification, or accreditation shall be stated.*

10.1.5.3.10 Government furnished property usage. This subparagraph shall be numbered 3.3.10 and shall specify any Government Furnished Equipment (GFE) to be incorporated into the system design. In addition, this paragraph shall specify any Government Furnished Information (GFI) and Government Furnished Software (GFS) to be incorporated into the system. This list shall identify the Government furnished property by reference to its nomenclature, specification number, and/or part number. If the list is extensive, it may be included as an appendix to this specification and referenced in this paragraph.

10.1.5.3.11 Computer resource reserve capacity. This subparagraph shall be numbered 3.3.11 and shall specify the required computer resource reserve capacity (e.g. memory, timing, etc.).

10.1.5.4 Documentation. This paragraph shall be numbered 3.4 and shall specify the requirements for system documentation such as specifications, drawings, technical manuals, test plans and procedures, and installation instruction data.

10.1.5.5 Logistics. This paragraph shall be numbered 3.5 and shall specify logistic considerations and conditions that apply to the operational requirements. These considerations and conditions may include:

- a. Maintenance
- b. Transportation modes
- c. Supply-system requirements
- d. Impact on existing facilities
- e. Impact on existing equipment.

10.1.5.6 Personnel and training. This paragraph shall be numbered 3.6 and be divided into the following subparagraphs to specify the requirements for personnel and training.

10.1.5.6.1 Personnel. This subparagraph shall be numbered 3.6.1 and shall specify personnel requirements which must be integrated into system design. These requirements shall be stated in terms of numbers plus tolerance and shall be the basis for contractor design and development decisions. Requirements stated in this paragraph shall be the basis for determination of system personnel training, training equipment, and training facility requirements. Personnel requirements shall include:

- a. Numbers and skills of support personnel for each operational deployment mode and the intended duty cycle, both normal and emergency.
- b. Skills and numbers of personnel that shall be allocated to the operation, maintenance, and control of the system.

10.1.5.6.2 Training. This subparagraph shall be numbered 3.6.2 and shall include the following training requirements:

- a. Contractor and Government responsibility for training. This subparagraph shall also specify the concept of how training shall be accomplished (e.g., school, contractor training).
- b. Equipment that will be required for training purposes.
- c. Training devices to be developed, characteristics of the training devices, and training and skills to be developed through the use of training devices.
- d. Training time and locations available for a training program.
- e. Source material and training aids to support the specified training.

10.1.5.7 Characteristics of subordinate elements. This paragraph shall be numbered 3.7 and shall be divided into the following subparagraphs to identify and describe each segment of the system. This subparagraph shall describe the relationships between the segments.

10.1.5.7.1 (Segment name and project unique identifier). This subparagraph shall be numbered 3.7.X (beginning with 3.7.1) and shall provide the following information for the segment:

- a. State the purpose of the segment
- b. Provide a brief description of the segment
- c. Identify the system capabilities the segment performs.

10.1.5.8 Precedence. This paragraph shall be numbered 3.8 and shall either specify the order of precedence of the requirements or assign weights to indicate the relative importance of the requirements.

10.1.5.9 Qualification. This paragraph shall be numbered 3.9 and shall state the requirements for verification or validation, as applicable, of capabilities in a specific application. Each qualification test shall be identified in a separate subparagraph and the specific application shall be described. Requirements shall be included for the conditions of testing, the time (program phase) of testing, period of testing, number of items to be tested, and any other pertinent qualification requirements. *This paragraph shall describe the approach to satisfying the relevant qualification requirements (such as testing, and verification, as applicable depending on the TCSEC level of the system) that are imposed by the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements.*

10.1.5.10 Standard sample. This paragraph shall be numbered 3.10 and, if applicable, shall describe requirements for the production of one or more standard samples. Standard samples shall be limited to the illustration of qualities and characteristics that cannot be described using detailed test procedures or design data or that cannot be definitively expressed.

10.1.5.11 Preproduction sample, periodic production sample, pilot, or pilot lot. This paragraph shall be numbered 3.11 and, if applicable, shall describe requirements for producing a preproduction or periodic production sample, a pilot model, or a pilot lot.

10.1.6 Quality assurance provisions. This section shall be numbered 4 and shall be divided into the following paragraphs to specify the requirements to show how the requirements of sections 3 and 5 shall be satisfied.

10.1.6.1 Responsibility for inspection. This paragraph shall be numbered 4.1 and shall assign responsibilities for performance of inspections of delivered products, materials, or services for determining compliance with all specified requirements.

10.1.6.2 Special tests and examinations. This paragraph shall be numbered 4.2 and shall specify any special tests and examinations required for sampling, lot formation, qualification evaluation, and any other tests or examinations as necessary. Each test and examination shall be described in a separate subparagraph. *This paragraph shall specify penetration testing as a special test, if penetration testing is applicable for the TCSEC level of the system.*

10.1.6.3 Requirements cross reference. This paragraph shall be numbered 4.3 and shall correlate each system requirement in sections 3 and 5 to the quality assurance provisions specified in section 4. This paragraph may reference a requirements cross reference table which may be provided as an appendix to this specification.

10.1.7 Preparation for delivery. This section shall be numbered 5 and shall specify requirements for the preparation of the system and all its components for delivery, including packaging and handling. This section shall include requirements to document any non-standard practices in appropriate system end item specifications. This section may impose requirements to comply with standard practice by referencing appropriate military specifications and standards to be used as the basis for preparing Section 5 of each specification for system end items.

10.1.8 Notes. This section shall be numbered 6 and shall contain any general information that aids in understanding this document (e.g., background information, glossary). This section shall contain an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document.

10.1.8.1 Intended use. This paragraph shall be numbered 6.1 and shall briefly state the purpose of the system to which the SSS applies in terms of the mission and threat addressed by the system.

10.1.8.1.1 Missions. This subparagraph shall be numbered 6.1.1 and shall describe the missions of the system to the extent that such missions affect design requirements. This description shall include operational information, such as tactics, system deployment, operating locations, and facilities.

10.1.8.1.2 Threat. This subparagraph shall be numbered 6.1.2 and shall describe the characteristics of potential targets, the characteristics of current and potential enemy weapon capabilities relevant to the system, and any additional threat considerations that affect the system design. This information may be contained in a separate document and referenced in this subparagraph if it is classified.

10.1.9 Appendixes. Appendixes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.), and the paragraphs within each appendix be numbered as multiples of 10 (e.g., Appendix A, paragraph 10, 10.1, 10.2, 20, 20.1, 20.2, etc.). Pages within each appendix shall be numbered alpha-numerically as follows: Appendix A pages shall be numbered A-1, A-2, A-3, etc. Appendix B pages shall be numbered B-1, B-2, B-3, etc.

DATA ITEM DESCRIPTION

SYSTEM/SEGMENT DESIGN DOCUMENT

DI-CMAN-80534-SDE

3. DESCRIPTION/PURPOSE

3.1 The System/Segment Design Document (SSDD) describes the design of a system/segment and its operational and support environments. It describes the organization of a system or segment as composed of Hardware Configuration Items (HWCI's), Computer Software Configuration Items (CSCI's), and manual operations.

(continued on page 2)

880229

EC

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for data generated under the work tasks described by paragraph 5.1.2.2 of DOD-STD-2167A.

7.2 The Contract Data Requirements List should specify whether this document is to be prepared and delivered on bound 8 1/2 by 11 inch bond paper or electronic media. If electronic media is selected, the precise format must be specified.

(continued on page 2)

N4329

10. PREPARATION INSTRUCTIONS

10.1 Content and format instructions. Production of this document using automated techniques is encouraged. Specific content and format instructions for this document are identified below.

- a. Response to tailoring instructions. In the event that a paragraph or subparagraph has been tailored out, a statement to that effect shall be added directly following the heading of each such (sub)paragraph. If a paragraph and all of its subparagraphs are tailored out, only the highest level paragraph heading need be included.
- b. Use of alternate presentation styles. Charts, tables, matrices, or other presentation styles are acceptable when the information required by the paragraphs and subparagraphs of this DID can be made more readable.
- c. Page numbering. Each page prior to Section 1 shall be numbered in lower-case roman numerals beginning with page ii for the Table of Contents. Each page starting from Section 1 to the appendixes shall be consecutively numbered in arabic numerals. If the document is divided into volumes, each such volume shall restart the page numbering sequence.

(continued on page 2)

DISTRIBUTION STATEMENT A.

Approved for public release; distribution is unlimited.

3. DESCRIPTION/PURPOSE (continued)

3.2 The SSDD contains the highest level design information for the system or segment. The SSDD describes the allocation of system requirements to HWCI, CSCI, and manual operations.

3.3 The SSDD describes the characteristics of each HWCI and CSCI to the Government.

3.4 The SSDD is used by the contractor for two primary purposes, namely: (1) present the system design at the System Design Review, (2) use the design information as the basis for developing the Software Requirements Specification for each CSCI, the Interface Requirements Specifications for the system, and the requirements specification for each HWCI.

3.5 The SSDD is used by the government to assess the design of a system or segment. The SSDD provides an overview of the system or segment that may also be used by training personnel, support personnel, or users of the system.

7. APPLICATION/INTERRELATIONSHIP (continued)

7.3 The SSDD is used to document the design of a system or a segment specified by an SSS, DI-CMAN-80008A. The word "system" is used generically in this DID to mean either a system or segment, as applicable.

10. PREPARATION INSTRUCTIONS (continued)

d. Document control numbers. For hardcopy formats, this document may be printed on one or both sides of each page (single-sided/double-sided). All printed pages shall contain the document control number and the date of the document centered at the top of the page. Document control numbers shall include revision and volume identification as applicable.

e. Multiple (sub)paragraphs. All paragraphs and subparagraphs starting with the phrase "This (sub)paragraph shall..." may be written as multiple subparagraphs to enhance readability. These subparagraphs shall be numbered sequentially.

f. Identifiers. The letter "X" serves as an identifier for a series of descriptions. For example, the paragraphs described by 10.1.6.2.1 shall be structured as follows:

4.2.1 (First CSCI name and identifier)

4.2.2 (Second CSCI name and identifier)

4.2.3 etc.

g. Document structure This document shall consist of the following:

- (1) Cover
- (2) Title page
- (3) Table of contents
- (4) Scope
- (5) Referenced documents
- (6) Operational concepts
- (7) System design

- (8) Processing resources
- (9) Quality factor compliance
- (10) Requirements traceability
- (11) Notes
- (12) Appendixes

10.1.1 Title page. The title page shall contain the information identified below in the indicated format:

[Document control number and date: Volume x of y (if multi-volume)]
 [Rev. indicator: date of Rev.]

SYSTEM DESIGN DOCUMENT
 (OR SEGMENT DESIGN DOCUMENT)

FOR THE

[SYSTEM NAME]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

Prepared for:

Contracting Agency Name, department code]

Prepared by:

[contractor name and address]

10.1.2 Table of contents. This document shall contain a table of contents listing the title and page number of each titled paragraph and subparagraph. The table of contents shall then list the title and page number of each figure, table, and appendix. in that order.

10.1.3 Scope. This section shall be numbered 1 and shall be divided into the following paragraphs.

10.1.3.1 Identification. This paragraph shall be numbered 1.1 and shall contain the approved identification number, title, and abbreviation, if applicable, of the system to which this SSDD applies. This paragraph shall identify the higher-level specification(s) containing the requirements from which the design of the system was derived.

10.1.3.2 System overview. This paragraph shall be numbered 1.2 and shall briefly state the purpose of the system to which this SSDD applies. *This overview shall identify the trust-related aspects of the system's purpose.*

10.1.3.3 Document overview. This paragraph shall be numbered 1.3 and shall summarize the purpose and contents of this document.

10.1.4 Referenced documents. This section shall be numbered 2 and shall list by document number and title all documents referenced in this document. This section shall also identify the source for all documents not available through normal Government stocking activities.

10.1.5 Operational Concepts. This section shall be numbered 3 and shall be divided into the following paragraphs and subparagraphs to describe the operational concepts of the system.

10.1.5.1 Mission. This subparagraph shall be numbered 3.1 and shall be divided into the following subparagraphs.

10.1.5.1.1 User needs. This subparagraph shall be numbered 3.1.1, shall summarize the user needs that are to be met by the system and shall reference the document(s) in which these needs are stated.

10.1.5.1.2 Primary mission(s). This subparagraph shall be numbered 3.1.2 and shall describe the primary mission(s) of the system.

10.1.5.1.3 Secondary mission(s). This subparagraph shall be numbered 3.1.3 and shall describe the secondary mission(s) of the system.

10.1.5.2 Operational environment. This paragraph shall be numbered 3.2 and shall describe the environment in which the system is intended to be employed.

10.1.5.3 Support environment. This paragraph shall be numbered 3.3 and shall describe the support environment for the operational system during the Production and Deployment phase of the system life cycle.

10.1.5.3.1 Support concept. This subparagraph shall be numbered 3.3.1 and shall describe the support concept for the system. This subparagraph shall include the following:

- (a) Use of multipurpose or automated test equipment
- (b) Repair versus replacement criteria
- (c) Levels of maintenance
- (d) Maintenance and repair cycles
- (e) Government and contractor support
- (f) Accessibility
- (g) Other.

10.1.5.3.2 Support facilities. This subparagraph shall be numbered 3.3.2 and shall describe the system support facilities and equipment to be used during the Production and Deployment phase of the system life cycle. A quantitative description of existing facilities and equipment shall be provided in sufficient detail so that their availability may be verified. A quantitative description of new or modified facilities and equipment shall be provided in sufficient detail to permit planning for construction or procurement.

10.1.5.3.3 Supply. This subparagraph shall be numbered 3.3.3 and shall describe the supply system, the impact of system requirements on the supply system, and the influence of the supply system on system design and use. This subparagraph shall include:

- (a) Introduction of new items into the supply system.
- (b) Re-supply methods.
- (c) Distribution and location of system stocks.

10.1.5.3.4 Government agencies. This paragraph shall be numbered 3.3.4 and shall identify the Government organizations that will be the development, support, and user agencies for the system.

10.1.5.4 System architecture. This paragraph shall be numbered 3.4 and shall describe the internal structure of the system. The segments, HWCI, and CSCI shall be identified and their purpose summarized. The relationships among the segments, HWCI, and CSCI shall be described. This paragraph shall also identify and state the purpose of each external interface of the system. A system architecture diagram may be used to illustrate the system top-level architecture. *The summary of purpose of each HWCI and CSCI shall identify the trust-related aspects of the purpose, and whether the HWCI or CSCI has any trust-related functional requirements. This shall be indicated in the architecture diagram, if possible. Segment relationship descriptions shall indicate what effect, if any, trust requirements will have on the relationship. Each statement of purpose of system external interface shall state what trusted-related functionality is provided by that interface, if any.*

10.1.5.5 Operational scenarios. This paragraph shall be numbered 3.5 and shall describe each operational scenario of the system. For each system state and mode, this paragraph shall identify the configuration items that execute and the manual operations to be performed. A table may be provided to illustrate the states and modes in which each configuration item executes and each manual operation is performed. In addition this paragraph shall describe the general flow of both execution control and data between configuration items while operating in the different states and modes. Flow diagrams may be used to illustrate execution control and data flow in each state and mode.

10.1.6 System design. This section shall be numbered 4 and shall be divided into the following paragraphs and subparagraphs to identify each HWCI, CSCI, and manual operation of the system. This section shall identify the HWCI(s) within the system that are to be designated as Prime Item(s) or Critical Item(s). A description of the relationship of HWCI, CSCI, and manual operations within the system shall be provided. A specification tree diagram(s) shall be used to describe the relationships between configuration items.

10.1.6.1 HWCI identification. This paragraph shall be numbered 4.1 and shall be divided into subparagraphs to identify the system requirements allocated to each HWCI.

10.1.6.1.1 (HWCI name and project-unique identifier). This subparagraph shall be numbered 4.1.X (beginning with 4.1.1), shall identify a HWCI by name and project-unique identifier, and shall state its purpose. This subparagraph shall identify each requirement from the System/Segment Specification allocated to the HWCI and the name and project-unique identifier of each system capability addressed by the HWCI. This subparagraph shall identify each interface external to the system addressed by the HWCI. Each interface external to the system shall be described in detailed quantitative terms (e.g., input/output voltages, dimensions, tolerances, loads, speeds, etc.). This subparagraph shall describe any design constraints on the HWCI.

This subparagraph shall identify each trust-related requirement of the HWCI.

10.1.6.2 CSCI identification. This paragraph shall be numbered 4.2 and shall be divided into subparagraphs to identify the system requirements allocated to each CSCI.

10.1.6.2.1 (CSCI name and project-unique identifier). This subparagraph shall be numbered 4.2.X (beginning with 4.2.1), shall identify a CSCI by name and project-unique identifier, and shall state its purpose. This subparagraph shall identify each requirement from the System/Segment Specification allocated to the CSCI and the name and project-unique identifier of each system capability addressed by the CSCI. This subparagraph shall identify each interface external to the system addressed by the CSCI. Each interface external to the system shall be described in detailed quantitative terms (e.g., bits per second, word length, message format, frequency of messages, priority rules, protocol). This subparagraph shall describe any design constraints on the CSCI. *This subparagraph shall identify each trust-related requirement of the CSCI.*

10.1.6.3 Manual operations identification. This paragraph shall be numbered 4.3 and shall be divided into subparagraphs to identify system requirements allocated to each manual operation.

10.1.6.3.1 (Manual operation name and project-unique identifier). This subparagraph shall be numbered 4.3.X (beginning with 4.3.1), shall identify a manual operation by name and project-unique identifier, and shall state its purpose. This subparagraph shall describe any design constraints that affect the manual operation and shall identify by name and project-unique identifier the capabilities from the System/Segment Specification to be satisfied by the manual operation.

10.1.6.4 Internal interfaces. This paragraph shall be numbered 4.4 and shall be divided into the following subparagraphs to describe the interfaces that are internal to the system. This paragraph shall depict the relationship of the interfaces to the configuration items in the system. This subparagraph may reference a system internal interface diagram.

10.1.6.4.1 (HWCI-to-HWCI interface name and project-unique identifier). This subparagraph shall be numbered 4.4.1 and shall identify by name and project-unique identifier all HWCI-to-HWCI interfaces within the system. This subparagraph shall identify each signal transmitted between HWCI's, the HWCI transmitting the signal, and the HWCI receiving the signal.

10.1.6.4.2 (HWCI-to-CSCI interface name and project-unique identifier). This subparagraph shall be numbered 4.4.2 and shall specify by name and project-unique identifier all HWCI-to-CSCI interfaces within the system. This subparagraph shall identify each signal transmitted between a CSCI and an HWCI, the HWCI or CSCI transmitting the signal, and the HWCI or CSCI receiving the signal.

10.1.6.4.3 (CSCI-to-CSCI interface name and project-unique identifier). This subparagraph shall be numbered 4.4.3 and shall specify by name and project-unique identifier all CSCI-to-CSCI interfaces within the system. This subparagraph shall identify each data item transmitted between CSCI's, the CSCI transmitting the data, and the CSCI receiving the data.

10.1.7 Processing resources. This section shall be numbered 5 and shall be divided into the following paragraphs to describe the processing resources for the system.

10.1.7.1 (Processing resource name and project-unique identifier). This paragraph shall be numbered 5.X (beginning with 5.1) and shall identify a processing resource by name and project-unique identifier. This paragraph shall identify the configuration items that use the resource. For each processing

resource, this paragraph shall specify the hardware, programming, design, coding, and utilization characteristics of the processing resource. In addition, this paragraph shall define the following computer hardware characteristics of the processing resource, as applicable:

- a. Memory size. Amount of internal memory (absolute, spare, or both) of the computer.
- b. Word size. Number of bits in each computer word.
- c. Processing speed. Computer processor capacity (absolute, spare, or both) (e.g., a twenty percent reserve when in the full operational configuration).
- d. Character set standard. Character set standard (e.g., ASCII, EBCDIC).
- e. Instruction set architecture. Instruction set architecture.
- f. Interrupt capabilities. Interrupt capabilities of the hardware.
- g. Direct Memory Access (DMA). Data transfer by DMA.
- h. Channel requirements. Channels and channel capacities (absolute, spare, or both).
- i. Auxiliary storage. Auxiliary storage capacities (absolute, spare, or both).
- j. Growth capabilities. Growth capability of any part of the processing resource.
- k. Diagnostic capabilities. Diagnostic capabilities.
- l. Additional computer hardware capabilities. Any additional computer hardware capabilities not previously mentioned (e.g., fault tolerance, preprocessing, floating point, array processor).
- m. Processing resource allocation. The allocation of pertinent processing resources to each CSCI.

10.1.8 Quality factor compliance. This section shall be numbered 6 and shall be divided into paragraphs and subparagraphs, as appropriate, to specify the models (and associated evaluation criteria) to be used to measure compliance with quality factor requirements.

10.1.9 Requirements traceability. This section shall be numbered 7 and shall provide traceability of the requirements allocated to the HWICs, CSCIs, and manual operations back to the requirements of the System/Segment Specification. The traceability may be shown in a requirements traceability matrix.

10.1.10 Notes. This section shall be numbered 8 and shall contain any general information that aids in understanding this document (e.g., background information, glossary, formula derivations). This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document.

10.1.11 Appendixes. Appendixes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.), and the paragraphs within each appendix be numbered as multiples of 10 (e.g., Appendix A, paragraph 10, 10.1, 10.2, 20, 20.1, 20.2, etc.). Pages within each appendix shall be numbered alpha-numerically as follows: Appendix A pages shall be numbered A-1, A-2, A-3, etc. Appendix B pages shall be numbered B-1, B-2, B-3, etc.

DATA ITEM DESCRIPTION

SOFTWARE REQUIREMENTS SPECIFICATION DI-CMAN-800025A-SDE

3. DESCRIPTION/PURPOSE

3.1 The Software Requirements Specification (SRS) specifies the engineering and qualification requirements for a Computer Software Configuration Item (CSCI).

3.2 The SRS is used by the contractor as the basis for the design and formal testing of a CSCI.

(continued on page 2)

880229

EC

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for data generated under the work tasks described by paragraphs 4.2.10, 5.1.2.3, 5.1.3, 5.2.2.1 and 5.2.3 of DOD-STD-2167A, 3.4.2 and 3.4.7.1 of MIL-STD-483, and 3.1.3.2.5.1 of MIL-STD-490.

7.2 The Contract Data Requirements List should specify whether this document is to be prepared and delivered on bound 8 1/2 by 11 inch bond paper or electronic media. If electronic media is selected, the precise format must be specified.

(continued on page 2)

N4340

10. PREPARATION INSTRUCTIONS

10.1 Content and format instructions. Production of this specification using automated techniques is encouraged. Specific content and format instructions for this specification are identified below.

- a. Response to tailoring instructions. In the event that a paragraph or subparagraph has been tailored out, a statement to that effect shall be added directly following the heading of each such (sub)paragraph. If a paragraph and all of its subparagraphs are tailored out, only the highest level paragraph heading need be included.
- b. Use of alternate presentation styles. Charts, tables, matrices, or other presentation styles are acceptable when the information required by the paragraphs and subparagraphs of this DID can be made more readable.
- c. Page numbering. Each page prior to Section 1 shall be numbered in lower-case roman numerals beginning with page ii for the Table of Contents. Each page starting from Section 1 to the beginning of the appendixes shall be consecutively numbered in arabic numerals. If the document is divided into volumes, each such volume shall restart the page numbering sequence.

(continued on page 2)

DISTRIBUTION STATEMENT A.

Approved for public release; distribution is unlimited.

3. DESCRIPTION/PURPOSE (continued)

3.3 The SRS specifies the requirements allocated to a CSCI and enables the Government to assess whether the completed CSCI complies with those requirements. Upon Government approval and authentication, the SRS becomes part of the Allocated Baseline.

7. APPLICATION/INTERRELATIONSHIP (continued)

7.3 The SRS is used to provide the detailed requirements for a CSCI specified in the System/Segment Specification, DI-CMAN-80008A, or Configuration Item Development Specification, DI-E-3102A.

7.4 The SRS may be used to specify requirements for an elaborate data base, such as a relational database. Requirements for such a database shall be specified in terms of a capability for which input and output requirements are to be interpreted as the data base contents requirements. When a database is shared by CSCIs, the requirements for the database shall be documented in one SRS and referenced in the SRSs of the sharing CSCIs. Any CSCI unique data element requirements for a database shall be documented in the SRS for that CSCI.

7.5 This DID supersedes DI-MCCR-80025 dated 4 June 1985.

10. PREPARATION INSTRUCTIONS (continued)

- d. Document control numbers. For hardcopy formats, this document may be printed on one or both sides of each page (single-sided/double-sided). All printed pages shall contain the document control number and the date of the document centered at the top of the page. Document control numbers shall include revision and volume identification as applicable.
- e. Multiple (sub)paragraphs. All paragraphs and subparagraphs starting with the phrase "This (sub)paragraph shall..." may be written as multiple subparagraphs to enhance readability. These subparagraphs shall be numbered sequentially.
- f. Identifiers. The letter "X" serves as an identifier for a series of descriptions. For example, the subparagraphs described by 10.1.5.2.1 shall be structured as follows:

- 3.2.1 (Name and identifier of the first capability)
- 3.2.2 (Name and identifier of the second capability)
- 3.2.3 etc.

- g. Document structure. This specification shall consist of the following:

- (1) Cover
- (2) Title page
- (3) Table of contents
- (4) Scope
- (5) Applicable documents
- (6) Engineering requirements

- (7) Qualification requirements
- (8) Preparation for delivery
- (9) Notes
- (10) Appendixes.

10.1.1 Title page. The title page shall contain the information identified below in the indicated format:

[Document control number and date: Volume x of y (if multi-volume)]
[Rev. indicator: date of Rev.]

SOFTWARE REQUIREMENTS SPECIFICATION

FOR THE

[CSCI NAME]

OF

[SYSTEM NAME]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

Prepared for:

[Contracting Agency Name, department code]

Prepared by:

[contractor name and address]

Authenticated by _____ Approved by _____
(Contracting agency) (Contractor) Date _____
Date _____

10.1.2 Table of contents. This specification shall contain a table of contents listing the title and page number of each titled paragraph and subparagraph. The table of contents shall then list the title and page number of each figure, table, and appendix, in that order.

10.2.3 Scope. This section shall be numbered 1 and shall be divided into the following paragraphs.

10.1.3.1 Identification. This paragraph shall be numbered 1.1 and shall contain the approved identification number, title, and if applicable, abbreviation of the system and the CSCI to which this SRS applies.

10.1.3.2 CSCI overview. This paragraph shall be numbered 1.2, shall briefly state the purpose of the system and shall identify and describe the role, within the system, of the CSCI to which this SRS applies.

10.1.3.3 Document overview. This paragraph shall be numbered 1.3 and shall summarize the purpose and contents of this document.

10.1.4 Applicable documents. This section shall be numbered 2 and shall be divided into the following paragraphs.

10.1.4.1 Government documents. This paragraph shall be numbered 2.1 and shall begin with one of the following two paragraphs: (1) "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement." (2) "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement, except for specification (enter number of next higher tiered specification) listed below." The following paragraph shall appear at the conclusion of the list of documents: "Copies of specifications, standards, drawings, and publications required by suppliers in connection with specified procurement functions should be obtained from the contracting agency or as directed by the contracting officer." Government documents shall be listed by document number and title in the following order:

SPECIFICATIONS:

- Federal
- Military
- Other Government Agency

STANDARDS:

- Federal
- Military
- Other Government Agency

DRAWINGS:

(Where detailed drawings referred to in a specification are listed on an assembly drawing, it is only necessary to list the assembly drawing.)

OTHER PUBLICATIONS:

- Manuals
- Regulations
- Handbooks
- Bulletins
- etc.

10.1.4.2 Non-Government documents. This paragraph shall be numbered 2.2 and shall begin with the following paragraph: "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement." The source for all documents not available through normal Government stocking activities shall be

listed. The following paragraph shall be placed at the conclusion of the list when applicable: "Technical society and technical association specifications and standards are generally available for reference from libraries. They are also distributed among technical groups and using Federal Agencies." Non-Government documents shall be listed by document number and title in the following order:

SPECIFICATIONS:

STANDARDS:

DRAWINGS:

OTHER PUBLICATIONS:

10.1.5 Engineering requirements. This section shall be numbered 3 and shall be divided into the following paragraphs and subparagraphs to specify the engineering requirements necessary to ensure proper development of the CSCI. Requirements to be included herein shall be allocated or derived from requirements established by the applicable SSS, PIDS, or CIDS.

10.1.5.1 CSCI external interface requirements. This paragraph shall be numbered 3.1 and shall identify the external interfaces of the CSCI. An external interface diagram similar to Figure 1 may be used to aid in this description. Each external interface shall be identified by name and project-unique identifier and a brief description of each interface shall be provided. *This description shall indicate whether the interface is related to any trust-related requirements.* Any identifying documentation, such as an Interface Control Document or Interface Requirements Specification, shall be referenced for each interface.

10.1.5.2 CSCI capability requirements. This paragraph shall be numbered 3.2 and shall identify, in the subparagraphs that follow, all of the capability requirements that the CSCI must satisfy. If the system of which the CSCI is a part can exist in various system states and modes as documented in the system specification, this paragraph shall identify each such state and mode and shall correlate each CSCI capability to those states and modes. A table may be used to depict this correlation.

10.1.5.2.1 (Capability name and project-unique identifier). This subparagraph shall be numbered 3.2.X (beginning with 3.2.1), shall identify the CSCI capability by name and project-unique identifier and shall state the purpose of the capability and its performance in measurable terms. This subparagraph shall identify and state the purpose of each input and output associated with the capability. This subparagraph shall identify the allocated or derived requirements that the capability satisfies or partially satisfies. If the capability can be more clearly specified by decomposing it into constituent capabilities, the requirements for each constituent capability shall be provided as one or more subparagraphs. Each constituent capability shall be assigned a project-unique identifier that is derived from the identifier of the parent capability.

10.1.5.3 CSCI internal interfaces. This paragraph shall be numbered 3.3 and shall identify the interfaces between the capabilities identified above. Each internal interface shall be identified by name and project-unique identifier and a brief description of each interface shall be provided, including a summary of the information transmitted over the interface. Internal interface diagrams depicting data flow, control flow, and other relevant information may be used to aid in this description.

FIGURE 1. Example external interface diagram.

10.1.5.4 CSCI data element requirements. This paragraph shall be numbered 3.4 and shall specify the information identified below, as applicable.

a. For data elements internal to the CSCI:

- (1) Assign a project-unique identifier to the data element
- (2) Provide a brief description of the data element
- (3) Identify the Units of measure required for the data element, such as seconds, meters, kilohertz, etc.
- (4) Identify the limit/range of values required for the data element (for constants provide the actual value)
- (5) Identify the accuracy required for the data element.
- (6) Identify the precision or resolution required for the data element in terms of significant digits
- (7) For data elements of the CSCI's internal interfaces:
 - Identify the interface by name and project-unique identifier
 - Identify the source capability of the data element by name and project-unique identifier
 - Identify the destination capability of the data element by name and project-unique identifier.

b. For data elements of the CSCI's external interfaces:

- (1) Identify the data elements by project-unique identifier
- (2) Identify the interface by name and project-unique identifier
- (3) Identify the source or destination capability, as applicable, by name and project-unique identifier
- (4) Reference the Interface Requirements Specification in which the interface is specified.

10.1.5.5 Adaptation requirements. This paragraph shall be numbered 3.5 and shall be divided into the following subparagraphs to specify the requirements for adapting the CSCI to site-unique conditions and to changes in the system environment.

10.1.5.5.1 Installation-dependent data. This subparagraph shall be numbered 3.5.1 and shall describe the site-unique data required by each installation. Examples of such data are: site latitude and longitude, radar ranges and areas of coverage, and prescribed safety limits. In addition, this subparagraph shall identify the CSCI capabilities in which these data are used.

10.1.5.5.2 Operational parameters. This subparagraph shall be numbered 3.5.2 and shall describe parameters required by the CSCI that may vary within a specified range according to operational needs. Examples of such data are: allowable trajectory deviations, navigation set model numbers, airplane performance characteristics, interaction/isolation of sorties, missile performance characteristics. This subparagraph shall identify the CSCI capabilities in which these data are used.

10.1.5.6 Sizing and timing requirements. This paragraph shall be numbered 3.6 and shall specify the amount and, if applicable, location of internal and auxiliary memory and the amount of processing time allocated to the CSCI. This paragraph shall specify the resources required of both memory and the central processing unit (CPU) for the CSCI.

10.1.5.7 Safety requirements. This paragraph shall be numbered 3.7 and shall specify safety requirements that are applicable to the design of the CSCI, with respect to potential hazards to personnel, property, and the physical environment.

10.1.5.8 Security requirements. This paragraph shall be numbered 3.8 and shall specify security requirements that are applicable to the design of the CSCI, with respect to potential compromise of sensitive data. *This paragraph shall identify which of the CSCI's requirements are specified in the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements. Each of these requirements shall be identified by a name and a reference to a section of the appropriate requirements document.*

10.1.5.9 Design constraints. This paragraph shall be numbered 3.9 and shall specify other requirements that constrain the CSCI design, such as the use of a particular processing configuration, etc. *This paragraph shall identify the CSCI's design constraints that are derived from the requirements of the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements.*

10.1.5.10 Software quality factors. This paragraph shall be numbered 3.10 and shall be divided into subparagraphs, as appropriate, to specify each software quality factor identified in the contract or derived from a higher level specification. *Among the quality factors specified shall be any relevant quality factors (such as resistance to penetration) that are derived from the requirements of the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements. These quality factors shall be identified as derived from trust requirements.* For each quality factor required, the method of compliance shall be specified along with the requirements for that factor.

10.1.5.11 Human performance/human engineering requirements. This paragraph shall be numbered 3.11 and shall specify the applicable human factors engineering requirements for the CSCI. These requirements shall include, as applicable, considerations for:

- a. Human information processing capabilities and limitations
- b. Foreseeable human errors under both normal and extreme conditions
- c. Implications for the total system environment (include training, support, and operational environment).

10.1.5.12 Requirements traceability. This paragraph shall be numbered 3.12 and shall contain a mapping of the engineering requirements in this specification to the requirements applicable to this CSCI in the SSS, PIDS, or CIDS. *This paragraph shall identify the requirements that are trust-related.* This paragraph shall also provide a mapping of the allocation of the CSCI requirements from the SSS, PIDS, or CIDS to the engineering requirements in this specification.

10.1.6 Qualification requirements. This section shall be numbered 4 and shall be divided into the following paragraphs to specify the qualification methods and any special qualification requirements necessary to establish that the CSCI satisfies the requirements of sections 3 and 5.

10.1.6.1 Qualification methods. This paragraph shall be numbered 4.1 and shall specify the qualification methods to be used to ensure that the CSCI requirements of section 3 and 5 have been satisfied. *Among the qualification methods specified shall be any relevant qualification methods (such as formal methods of analysis) that are derived from the requirements of the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements. These qualification methods shall be identified as derived from trust requirements.* A table similar to Table I may be used to present this information. Qualification methods include:

- a. Demonstration. The operation of the CSCI (or some part of the CSCI) that relies on observable functional operation not requiring the use of elaborate instrumentation or special test equipment.

- b. Analysis. The processing of accumulated data obtained from other qualification methods. Examples are interpretation or extrapolation of test data.
- c. Inspection. The visual examination of CSCI code, documentation, etc.

TABLE I. Example of a qualification cross-reference table.

10.1.6.2 Special qualification requirements. This paragraph shall be numbered 4.2 and shall be divided into appropriate subparagraphs to specify special requirements associated with qualification of the CSCI. This paragraph shall identify and describe, if applicable, special tools, techniques (e.g., test formulas, algorithms), procedures, facilities, and acceptance limits. For each special test the following information shall be specified:

- a. A project-unique identifier for the test
- b. The paragraph number(s) of the capability requirement(s) to which the test applies
- c. A description of the test, such as peak-load stress test for 24 hr. duration
- d. The level of the test (CSU, CSC, CSCI, segment, or system level).

10.1.7 Preparation for delivery. This section shall be numbered 5 and shall specify the type and characteristics of the delivery media for the CSCI (e.g., 8 track magnetic tape 1600 BPI, 150 megabyte disk). In addition, this section shall specify the labeling, packaging, handling, and classification marking requirements for the media, including the CSCI name and project-unique identifier. Any unique delivery requirements shall also be specified in this section.

10.1.8 Notes. This section shall be numbered 6 and shall contain any general information that aids in understanding this specification (e.g., background information, glossary, formula derivations). This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document.

10.1.9 Appendixes. Appendixes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.), and the paragraphs within each appendix be numbered as multiples of 10 (e.g., Appendix A, paragraph 10, 10.1, 10.2, 20, 20.1, 20.2, etc.). Pages within each appendix shall be numbered alpha-numerically as follows: Appendix A pages shall be numbered A-1, A-2, A-3, etc. Appendix B pages shall be numbered B-1, B-2, B-3, etc.

DATA ITEM DESCRIPTION

INTERFACE REQUIREMENTS SPECIFICATION DI-CMAN-800026A-SDE

3. DESCRIPTION/PURPOSE

3.1 The Interface Requirements Specification (IRS) specifies the requirements for one or more interfaces between one or more Computer Software Configuration Items (CSCIs) and other configuration items or critical items.

(continued on page 2)

880229

EC

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for data generated under the work tasks described by paragraphs 5.1.2.4 and 5.2.2.2 of DOD-STD-2167A, 3.4.2 and 3.4.7.1 of MIL-STD-483, and 3.1.3.2.5.2 of MIL-STD-490.

7.2 The Contract Data Requirements List should specify whether this document is to be prepared and delivered on bound 8 1/2 by 11 inch bond paper or electronic media. If electronic media is selected, the precise format must be specified.

(continued on page 2)

N4341

10. PREPARATION INSTRUCTIONS

10.1 Content and format instructions. Production of this specification using automated techniques is encouraged. Specific content and format instructions for this specification are identified below.

- a. Response to tailoring instructions. In the event that a paragraph or subparagraph has been tailored out, a statement to that effect shall be added directly following the heading of each such (sub)paragraph. If a paragraph and all of its subparagraphs are tailored out, only the highest level paragraph heading need be included.
- b. Use of alternate presentation styles. Charts, tables, matrices, or other presentation styles are acceptable when the information required by the paragraphs and subparagraphs of this DID can be made more readable.
- c. Page numbering. Each page prior to Section 1 shall be numbered in lower-case roman numerals beginning with page ii for the Table of Contents. Each page starting from Section 1 to the beginning of the appendixes shall be consecutively numbered in arabic numerals. If the document is divided into volumes, each such volume shall restart the page numbering sequence.

(continued on page 2)

DISTRIBUTION STATEMENT A.

Approved for public release; distribution is unlimited.

3. DESCRIPTION/PURPOSE (continued)

3.2 The IRS specifies the requirements for the interface(s) and enables the Government to assess whether the implementation of the interface(s) complies with those requirements. Upon Government approval and authentication, the IRS becomes the joint configuration control device for the interface(s) and becomes part of the Allocated Baseline.

3.3 The IRS is used by the contractor(s) as the basis for development of the interface(s).

7. APPLICATION/INTERRELATIONSHIP (continued)

7.3 Detailed design information for the interface(s) defined by the IRS is provided in the Interface Design Document (IDD), DI-MCCR-80027A.

7.4 This DID supersedes DI-MCCR-80026 dated 4 June 1985.

10. PREPARATION INSTRUCTIONS (continued)

d. Document control numbers For hardcopy formats, this document may be printed on one or both sides of each page (single-sided/double-sided). All printed pages shall contain the document control number and the date of the document centered at the top of the page. Document control numbers shall include revision and volume identification as applicable.

e. Multiple (sub)paragraphs. All paragraphs and subparagraphs starting with the phrase "The (sub)paragraph shall..." may be written as multiple subparagraphs to enhance readability. These subparagraphs shall be numbered sequentially.

f. Identifiers. The letters "X" and "Y" serve as identifiers for a series of descriptions. For example, the subparagraphs described by 10.1.5.2 shall be structured as follows:

3.1 (Name and identifier of the first interface).

3.1.1 Interface requirements

3.1.2 Data requirements

3.2 (Name of the second interface).

3.2.1 Interface requirements

3.2.2 Data requirements

3.3 etc.

g. Document structure. This specification shall consist of the following:

- (1) Cover
- (2) Title page
- (3) Table of contents
- (4) Scope
- (5) Applicable documents

- (6) Interface specification
- (7) Notes
- (8) Appendixes.

10.1.1 Title page. The title page shall contain the information identified below in the indicated format:

[Document control number and date: Volume x of y (if multi-volume)]
 [Rev. indicator: date of Rev.]

INTERFACE REQUIREMENTS SPECIFICATION

FOR THE

[SYSTEM NAME]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

Prepared for:

[Contracting Agency Name, department code]

Prepared by:

[contractor name and address]

Authenticated by _____
 (Contracting agency)

Approved by _____
 (Contractor)

Date _____

Date _____

10.1.2 Table of contents. This specification shall contain a table of contents listing the title and page number of each titled paragraph and subparagraph. The table of contents shall then list the title and page number of each figure, table, and appendix, in that order.

10.1.3 Scope. This section shall be numbered 1 and shall be divided into the following paragraphs.

10.1.3.1 Identification. This paragraph shall be numbered 1.1 and shall contain the approved identification number and title of the interface(s) to which this IRS applies.

10.1.3.2 System overview. This paragraph shall be numbered 1.2 and shall briefly state the purpose of the system and shall identify and describe the role, within the system, of the interfaces to which this IRS applies.

10.1.3.3 Document overview. This paragraph shall be numbered 1.3 and shall summarize the purpose and contents of this document.

10.1.4 Applicable documents. This section shall be numbered 2 and shall be divided into the following paragraphs.

10.1.4.1 Government documents. This paragraph shall be numbered 2.1. This paragraph shall begin with one of the following two paragraphs, as applicable: (1) "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement." (2) "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement, except for specification (enter number of next higher-tiered specification) listed below." The following paragraph shall appear at the conclusion of the list of documents: "Copies of specifications, standards, drawings, and publications required by suppliers in connection with specified procurement functions should be obtained from the contracting agency or as directed by the contracting officer." Government documents shall be listed by document number and title in the following order:

SPECIFICATIONS:

- Federal
- Military
- Other Government Agency

STANDARDS:

- Federal
- Military
- Other Government Agency

DRAWINGS:

(Where detailed drawings referred to in a specification are listed on an assembly drawing, it is only necessary to list the assembly drawing.)

OTHER PUBLICATIONS:

- Manuals
- Regulations
- Handbooks
- Bulletins
- etc.

10.1.4.2 Non-Government documents. This paragraph shall be numbered 2.2 and shall begin with the following paragraph: "The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement." The source for all documents not available through normal Government stocking activities shall be listed. The following paragraph shall be placed at the conclusion of the list when applicable: "Technical society and technical association specifications and standards are generally available for reference from libraries. They are also distributed among technical groups and using Federal Agencies." Non-Government documents shall be listed by document number and title in the following order:

SPECIFICATIONS:**STANDARDS:****DRAWINGS:****OTHER PUBLICATIONS:**

10.1.5 Interface specification. This section shall be numbered 3 and shall be divided into the following paragraphs and subparagraphs to specify the requirements for those interfaces to which this IRS applies.

10.1.5.1 Interface diagrams. This paragraph shall be numbered 3.1 and shall identify the interfaces among the CSCIs, HWCI, and critical items to which this specification applies. One or more interface diagrams, as appropriate, shall be provided to depict the interfaces. Each interface shall be identified by name and project-unique identifier.

10.1.5.2 (Interface name and project-unique identified.) This paragraph shall be numbered 3.X (beginning with 3.2), shall identify an interface by name and project-unique identifier, and shall state its purpose. *This paragraph shall identify the requirements that are trust-related.* This paragraph shall be divided into the following subparagraphs to specify the requirements for the interface and for the data transmitted across the interface.

10.1.5.2.1 Interface requirements. This subparagraph shall be numbered 3.X.1 (beginning with 3.2.1) and shall specify the following, as applicable:

a. Whether the interfacing CSCIs are to execute concurrently or sequentially. If concurrently, the method of inter-CSCI synchronization to be used. b. The communication protocol to be used for the interface. c. The priority level of the interface.

10.1.5.2.2 Data requirements. This paragraph shall be numbered 3.X.2 (beginning with 3.2.2) and shall specify, in a data element definition table similar to Table I, the following information, as applicable, for each data element transmitted across the interface: *This paragraph shall describe any security-critical data elements.*

- a. A project-unique identifier for the data element
- b. A brief description of the data element
- c. The CSCI, HWCI, or critical item that is the source of the data element
- d. The CSCI(s), HWCI(s), or critical item(s) that are the users of the data element
- e. The Units of measure required for the data element, such as seconds, meters, kilohertz, etc.
- f. The limit/range of values required for the data element (for constants provide the actual value)
- g. The accuracy required for the data element
- h. The precision or resolution required for the data element in terms of significant digits.

10.1.6 Quality Assurance. This section shall be numbered 4 and shall state "NONE."

10.1.7 Preparation for delivery. This section shall be numbered 5 and shall state "NONE".

10.1.8 Notes. This section shall be numbered 6 and shall contain any general information that aids in understanding this document (e.g., background information, glossary, etc.). This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document.

10.1.9 Appendixes. Appendixes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.), and the paragraphs within each appendix be numbered as multiples of 10 (e.g., Appendix A, paragraph 10, 10.1, 10.2, 20, 20.1, 20.2, etc.). Pages within each appendix shall be numbered alpha-numerically as follows: Appendix A pages shall be numbered A-1, A-2, A-3, etc. Appendix B pages shall be numbered B-1, B-2, B-3, etc.

DATA ITEM DESCRIPTION

SOFTWARE DESIGN DOCUMENT

DI-MCCR-80012A-SDE

3. DESCRIPTION/PURPOSE

3.1 The Software Design Document (SDD) describes the complete design of a Computer Software Configuration Item (CSCI). It describes the CSCI as composed of Computer Software Components (CSCs) and Computer Software Units (CSUs).

(continued on page 2)

880229

EC

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for data generated under work tasks described by paragraphs 5.3.2.1, 5.3.2.3, 5.4.2.1, 5.4.2.3, and 5.7.2.1 of DOD-STD-2167A, 3.4.7.2 of MIL-STD-483, and 3.1.3.3.5.1 and 3.1.3.3.5.2 of MIL-STD-490.

7.2 The Contract Data Requirements List should specify whether this document is to be prepared and delivered on bound 8 1/2 by 11 inch bond paper or electronic media. If electronic media is selected, the precise format must be specified.

(continued on page 2)

N4330

10. PREPARATION INSTRUCTIONS

10.1 Content and format instructions. Production of this document using automated techniques is encouraged. Specific content and format instructions for this document are identified below.

- a. Response to tailoring instructions. In the event that a paragraph or subparagraph has been tailored out, a statement to that effect shall be added directly following the heading of each such (sub)paragraph. If a paragraph and all of its subparagraphs are tailored out, only the highest level paragraph heading need be included.
- b. Use of alternate presentation styles. Charts, tables, matrices, or other presentation styles are acceptable when the information required by the paragraphs and subparagraphs of this DID can be made more readable.
- c. Page numbering. Each page prior to Section 1 shall be numbered in lower-case roman numerals beginning with page ii for the Table of Contents. Each page starting from Section 1 to the beginning of the appendixes shall be consecutively numbered in arabic numerals. If the document is divided into volumes, each such volume shall restart the page numbering sequence.

(continued on page 2)

DISTRIBUTION STATEMENT A.

Approved for public release; distribution is unlimited.

3. DESCRIPTION/PURPOSE (continued)

3.2 The SDD describes the allocation of requirements from a CSCI to its CSCs and CSUs. Prior to Preliminary Design Review, the SDD is entered into the Developmental Configuration for the CSCI. Upon completion of Physical Configuration Audit (PCA), the SDD, as part of the Software Product Specification, is entered into the Product Baseline for the CSCI.

3.3 The SDD is used by the contractor for three primary purposes, namely: (1) present the preliminary design at the Preliminary Design Review(s), (2) present the detailed design at the Critical Design Review(s), and (3) use the design information as the basis for coding each CSU.

3.4 The SDD is used by the Government to assess the preliminary and detailed design of a CSCI.

7. APPLICATION/INTERRELATIONSHIP (continued)

7.3 An SDD is developed incrementally as follows:

- a. Sections 1, 2, 3, 7, and 8 are produced during preliminary design and are presented at Preliminary Design Review (PDR).
- b. Sections 4, 5, and 6 are produced during detailed design and all other sections are updated, as applicable. The complete SDD is presented at Critical Design Review (CDR).

7.4 In preparation for PCA, the SDD is incorporated into the Software Product Specification (SPS), DI-MCCR-80029A.

7.5 This DID supersedes DI-MCCR-80012, DI-MCCR-80028, and DI-MCCR-80031 dated 4 June 1985.

10. PREPARATION INSTRUCTIONS (continued)

- d. Document control numbers. For hardcopy formats, this document may be printed on one or both sides of each page (single-sided/double-sided). All printed pages shall contain the document control number and the date of the document centered at the top of the page. Document control numbers shall include revision and volume identification as applicable.
- e. Multiple (sub)paragraphs. All paragraphs and subparagraphs starting with the phrase "This (sub)paragraph shall..." may be written as multiple subparagraphs to enhance readability. These subparagraphs shall be numbered sequentially.
- f. Identifiers. The letters "X" and "Y" serve as identifiers for a series of descriptions. For example, the paragraphs and subparagraphs described by 10.1.6.1 shall be structured as follows:

4.1 (Name and identifier of the first CSC).

4.1.1 (Name and identifier of the first CSU)

4.1.2 (Name and identifier of the second CSU)

4.1.3 etc.

4.2 (Name and identifier of the second CSC).

4.2.1 etc.

g. Document structure. This document shall consist of the following:

- (1) Cover
- (2) Title page
- (3) Table of contents
- (4) Scope
- (5) Referenced documents
- (6) Preliminary design
- (7) Detailed design
- (8) CSCI data
- (9) CSCI data files
- (10) Requirements traceability
- (11) Notes
- (12) Appendixes.

10.1.1 Title page. The title page shall contain the information identified below in the indicated format:

[Document control number and date: Volume x of y (if multi-volume)]
 [Rev. indicator: date of Rev.]

SOFTWARE DESIGN DOCUMENT

FOR THE

[CSCI NAME]

OF

[SYSTEM NAME]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

Prepared for:

[Contracting Agency Name, department code]

Prepared by:

[contractor name and address]

10.1.2 Table of contents. This document shall contain a table of contents listing the title and page number of each titled paragraph and subparagraph. The table of contents shall then list the title and page number of each figure, table, and appendix, in that order.

10.1.3 Scope. This section shall be numbered 1 and shall be divided into the following paragraphs.

10.1.3.1 Identification. This paragraph shall be numbered 1.1 and shall contain the approved identification number, title, and abbreviation, if applicable, of the system and the CSCI to which this SDD applies. This paragraph shall identify the higher-level specification(s) containing the requirements from which the design of this CSCI was derived.

10.1.3.2 System overview. This paragraph shall be numbered 1.2 and shall briefly state the purpose of the system and the CSCI to which this SDD applies.

10.1.3.3 Document overview. This paragraph shall be numbered 1.3 and shall summarize the purpose and contents of this document.

10.1.4 Referenced documents. This section shall be numbered 2 and shall list by document number and title all documents referenced in the SDD. This section shall also identify the source for all documents not available through normal Government stocking activities.

10.1.5 Preliminary design. This section shall be numbered 3 and shall be divided into the following paragraphs to describe the preliminary design of the CSCI.

10.1.5.1 CSCI overview. This paragraph shall be numbered 3.1 and shall identify and describe the role of the CSCI within the system to which this SDD applies. The overview shall identify and state the purpose of each external interface of the CSCI. A system architecture diagram may be used to show the relationships between this CSCI and the other CIs in the system. *This overview shall identify and describe the trust-related aspects of the CSCI's role in the system, and of each of the CSCI's CSCI external interfaces. The description shall identify each CSCI external interface that is also a TCB interface.*

10.1.5.1.1 CSCI architecture. This paragraph shall be numbered 3.1.1 and shall describe the internal organizational structure of the CSCI. The Computer Software Components (CSCs) and sub-level CSCs shall be identified and their purpose summarized. The relationships among the CSCs shall be described. The relationship description shall identify and state the purpose of each CSC-to-CSC interface and shall summarize the data transmitted via the interface. This paragraph shall identify any non-developmental software to be incorporated into the CSCI. The CSCI top-level architecture may be illustrated graphically. *This paragraph shall identify the trust-related aspects of the purpose of each CSC and each CSC interface, and shall identify each CSC interface that is also a TCB interface.*

10.1.5.1.2 System states and modes. This paragraph shall be numbered 3.1.2 and shall identify each system state and mode in which the CSCI operates and the CSCs that execute in each state and mode. A state/CSC table may be provided to illustrate the system states and modes that each CSC executes. In addition, this paragraph shall describe the general flow of both execution control and data between CSCs while operating in the different states and modes. A flow diagram(s) may be used to illustrate the execution control and data flow in each state and mode.

10.1.5.1.3 Memory and processing time allocation. This paragraph shall be numbered 3.1.3 and shall document the allocation of memory and processing time to the CSCs. The allocation may be illustrated by a memory/processing time table (see Table I).

TABLE I. Example of a CSC memory/processing time table.

10.1.5.2 CSCI design description. This section shall be numbered 3.2 and shall be divided into the following subparagraphs to provide a design description of each CSC of the CSCI.

10.1.5.2.1 (CSC name and project unique identifier). This subparagraph shall be numbered 3.2.X (beginning with 3.2.1), shall identify a CSC by name and project unique identifier, and shall state its purpose, *including a description of the trust-related aspects of the purpose*. This subparagraph shall provide the following information:

- a. Identify the requirements allocated to the CSC from the applicable requirements specification(s). *Identify the requirements that are trust-related.* If the CSC is composed of sub-level CSCs, some or all of this information may be referenced and provided by the sub-level CSC description.
- b. Describe the preliminary design of the CSC in terms of execution control and data flow. *Identify the data-flow of security-critical data.* If a CSC is composed of sub-level CSCs, this description shall identify the relationships among the sub-level CSCs. In addition this description shall identify each CSCI internal interface documented in the Software Requirements Specification, that is to be addressed by the CSC and its sub-level CSCs, as applicable. This information may be referenced rather than duplicated for each sub-level CSC.
- c. Identify the derived design requirements for the CSC and any design constraints imposed on or by the CSC. *Identify the derived design requirements that are trust-related. Identify the design constraints (such as modularity for B2 and higher systems) that are derived from requirements of the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements.* If the CSC is composed of sub-level CSCs, some or all of this information may be referenced and provided by the sub-level CSC description.

10.1.5.2.1.1 (Sub-level CSC name and project unique identifier). This subparagraph shall be numbered 3.2.X.Y (beginning with 3.2.1.1), shall identify a sub-level CSC by name and project unique identifier, shall state its purpose, and shall provide the information required by a through c above. This subparagraph does not apply if there are no sub-level CSCs. If this CSC is also composed of sub-level CSCs, each sub-level CSC shall be identified by name and project unique identifier and the information required by a through c above shall be provided in a separate subparagraph for each sub-level CSC.

10.1.6 Detailed design. This section shall be numbered 4 and shall be divided into the following paragraphs and subparagraphs to describe the detailed design of each CSC.

10.1.6.1 (CSC name and project unique identifier). This paragraph shall be numbered 4.X (beginning with 4.1), and shall be divided into the following subparagraphs to identify and describe each of the Computer Software Units (CSUs) of a CSC. This paragraph shall describe the relationships of the CSUs in terms of execution control and data flow between the CSUs of this CSC and shall identify all CSU interfaces that are external to the CSC, *and shall identify all CSU interfaces that are TCB interfaces, and all data-flow of security-critical data.* Each CSU that is used by more than one CSC shall be described in detail under one CSC and then referenced by the other using CSCs.

10.1.6.1.2 (CSU name and project unique identifier). This subparagraph shall be numbered 4.X.Y (beginning with 4.1.1) and shall identify a CSU by name and project unique identifier and shall state the purpose of the CSU, *including the trust-related aspects of the CSU's purpose.* This subparagraph shall be divided into the following subparagraphs to provide the design information for the CSU.

10.1.6.1.2.1 (CSU name) Design specification/constraints. This subparagraph shall be numbered 4.X.Y.1 (beginning with 4.1.1.1) and shall state the design requirements for the CSU. This subparagraph shall identify the requirements allocated to the CSC that are to be satisfied or partially satisfied by the CSU and shall identify any constraints on the design of the CSU. *This subparagraph shall identify which requirements are trust-related, and which design and implementation constraints (such as modularity for B2 and higher systems) are derived from requirements of the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements.* The design requirements addressed in this subparagraph shall include design requirements for the man-machine interface, as applicable.

10.1.6.1.2.2 (CSU name) Design. This subparagraph shall be numbered 4.X.Y.2 (beginning with 4.1.1.2) and shall specify the design of the CSU. If the CSU is to be coded in a programming language other than the specified CSCI language, the programming language shall be identified and the rationale for its use shall be provided. If the CSU resides in a library, this subparagraph shall identify the library by name and project unique identifier, and the design document in which the library description can be found. The detailed design information identified below shall be provided for the CSU, as applicable. This information may be provided by automated tools or other techniques, such as a program design language, flowcharts, or other design representations. *This detailed design information shall identify and describe any aspects that are relevant to trust-related requirements, including but not limited to: security-critical algorithms (e.g. access mediation), handling of trust-related errors (e.g. authentication failure), protection-critical data structures, data files, or databases, and limitations imposed by trust requirements (e.g. resource usage driven by covert channel concerns).*

- a. **Input/output data elements.** Identify and state the purpose of each input and output data element to the CSU. The design information for data elements shall be provided in section 5.
- b. **Local data elements.** Identify and state the purpose of each data element that originates in the CSU and is not used by any other CSU. Each data element shall be described in terms of name, brief description, data type, data representation, size, units of measure, limit/range, accuracy, precision/resolution, and any other attributes of the data. This information may be provided in a CSU local data definition table.
- c. **Interrupts and signals.** Identify and describe the interrupts and signals handled by the CSU. Identify for each interrupt and signal, as appropriate, its source, purpose, priority, expected response and response time, and minimum, maximum, and probable frequency of occurrence.
- d. **Algorithms.** Identify, state the purpose, and describe in detail the algorithms to be incorporated into the execution of the CSU. The algorithms shall be described in terms of the manipulation of input and local data elements and the generation of output data elements.
- e. **Error handling.** Identify and describe the error detection and recovery features of the CSU, including handling of erroneous input data and other conditions that affect the execution of the CSU.
- f. **Data conversion.** Identify and describe any data conversion operations performed in order to implement the CSU's interfaces.
- g. **Use of other elements.** Describe the use of other elements that are used by the CSU including, but not limited to:
 - (1) Other CSUs (e.g., calls for library functions, calls for I/O services for access to databases, mass storage devices, and real-time I/O channels).
 - (2) Shared data stored in a global memory (e.g., databases or data files, tables, compool, datapool, etc.).
 - (3) Input and output buffers, including message buffers.

- h. **Logic flow.** Describe the logic flow of the CSU in terms of items "a" through "g" above. Describe the conditions under which CSU execution is initiated and, if applicable, communication interface features are invoked, and the conditions under which control is passed to other CSUs, as applicable. If sequencing is dynamically controlled during the CSCI's operations, the method for sequence control and the logic and input conditions of that method shall be described, such as timing variations, priority assignments, internal operations such as data transfer in and out of internal memory, sensing of discrete input signals, and timing relationships between interrupt operations with the CSCI.
- i. **Data structures.** Describe local data structures implemented by the CSU and any shared data structures used by the CSU. Shared data structures shall be described under one CSU and referenced thereafter by the sharing CSUs.
- j. **Local data files or database.** If a data file(s) or a database are part of the local data of a CSU, state the purpose of each file or database, the structure of each file or database in terms of records, fields, etc., and describe the access procedures, such as sequential or random.
- k. **Limitations.** Describe any limitations or unusual features that restrict the performance of the CSU.

10.1.7 CSCI data. This section shall be numbered 5 and shall describe the global data elements within the CSCI, *identifying those CSCI global data elements that are protection-critical*. For ease in readability and maintenance, the information required below may be provided in one or more tables. The following information shall be provided for each data element, as applicable:

a. For data elements internal to the CSCI:

- (1) Name of the data element
- (2) A brief description
- (3) The units of measure, such as knots, seconds, meters, feet, etc.
- (4) The limit/range of values required for the data element (for constants provide the actual value)
- (5) The accuracy required for the data element
- (6) The precision/resolution in terms of significant digits
- (7) For real time systems, the frequency at which the data element is calculated or refreshed, such as 10 KHz, 50 Msec, etc.
- (8) Legality checks performed on the data element
- (9) The data type, such as integer, ASCII, fixed, real, enumeration, etc.
- (10) The data representation/format
- (11) The CSU project unique identifier where the data element is set or calculated
- (12) The CSU project unique identifier(s) where the data element is used
- (13) The data source from which the data is supplied, such as database or data file, global common, local common, compool, datapool, parameter, etc. Where applicable, each source shall be identified by its project unique identifier.

b. For data elements of the CSCI's external interfaces:

- (1) Identify the data element
- (2) Identify the interface by name and project unique identifier
- (3) Reference the Interface Design Document (IDD) in which the external interface is described.

10.1.3 CSCI data files. This section shall be numbered 6 and shall be divided into the following paragraphs to describe each of the shared data files of the CSCI. *These paragraphs shall identify the security-critical data in the database.*

10.1.8.1 Data file to CSC/CSU cross reference. This paragraph shall be numbered 6.1 and shall provide a mapping of each data file identified below to the CSCs and CSUs that use the data file.

10.1.8.2 (Data file name and project unique identifier). This subparagraph shall be numbered 6.X (beginning with 6.2) and shall identify by name and project unique identifier a data file of the CSCI that is shared by more than one CSU. This paragraph shall state the purpose of the data file, identify the maximum size of the file, and describe the file access method, such as random or sequential. This paragraph shall provide a description of the structure and size of the records contained within the file. This paragraph shall also provide a description of the data that is to reside in the file. The data description shall include, as applicable, data type, data representation, size, units of measure, limit/range, accuracy, precision/resolution, and any other design characteristics of the data. This information may be provided in a file definition table.

10.1.9 Requirements traceability. This section shall be numbered 7 and shall provide traceability of the requirements allocated down to the CSU level of each CSC back to the requirements of the Software Requirements Specification and Interface Requirements Specification. The traceability may be shown graphically.

10.1.10 Notes. This section shall be numbered 8 and shall contain any general information that aids in understanding this document (e.g., background information, glossary, formula derivations). This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document.

10.1.11 Appendixes. Appendixes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.), and the paragraphs within each appendix be numbered as multiples of 10 (e.g., Appendix A, paragraph 10, 10.1, 10.2, 20, 20.1, 20.2, etc.). Pages within each appendix shall be numbered alpha-numerically as follows: Appendix A pages shall be numbered A-1, A-2, A-3, etc. Appendix B pages shall be numbered B-1, B-2, B-3, etc.

10.1.11.1 Detailed Top-Level Specification. *There shall be an appendix which summarizes the detailed top-level specification of the CSCI, by enumerating all the TCB interfaces provided by the CSCI, and cross-references each to the CSU section that describes the interface.*

DATA ITEM DESCRIPTION

INTERFACE DESIGN DOCUMENT

DI-MCCR-80027A-SDE

3. DESCRIPTION/PURPOSE

3.1 The Interface Design Document (IDD) specifies the detailed design for one or more interfaces between one or more Computer Software Configuration Items (CSCIs) and other configuration items or critical items.

(continued on page 2)

880229

EC

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for that data generated under word tasks described by 5.3.2.2, 5.4.2.2, and 5.7.2.2 of DOD-STD-2167A, 3.4.7.2 of MIL-STD-483, and 3.1.3.3.5.4 of MIL-STD-490.

7.2 The Contract Data Requirements List should specify whether this document is to be prepared and delivered on bound 8 1/2 by 11 inch bond paper or electronic media. If electronic media is selected, the precise format must be specified.

(continued on page 2)

N4342

10. PREPARATION INSTRUCTIONS

10.1 Content and format instructions. Production of this document using automated techniques is encouraged. Specific content and format instructions for this document are identified below.

- a. Response to tailoring instructions. In the event that a paragraph or subparagraph has been tailored out, a statement to that effect shall be added directly following the heading of each such (sub)paragraph. If a paragraph and all of its subparagraphs are tailored out, only the highest level paragraph heading need be included.
- b. Use of alternate presentation styles. Charts, tables, matrices, or other presentation styles are acceptable when the information required by the paragraphs and subparagraphs of this DID can be made more readable.
- c. Page numbering. Page numbering. Each page prior to Section 1 shall be numbered in lower-case roman numerals beginning with page ii for the Table of Contents. Each page starting from Section 1 to the beginning of the appendixes shall be consecutively numbered in arabic numerals. If the document is divided into volumes, each such volume shall restart the page numbering sequence.

(continued on page 2)

DISTRIBUTION STATEMENT A.

Approved for public release; distribution is unlimited.

3. DESCRIPTION/PURPOSE (continued)

3.2 The IDD and its companion Interface Requirements Specification (IRS) serve to communicate and control interface design decisions to the Government. Upon completion of Physical Configuration Audit, the IDD becomes a part of the Product Baseline.

3.3 The IDD is used by the contractor(s) as the basis for software design of the interface(s).

3.4 The IDD is used by the Government to assess the design of the interfaces documented in the Interface Requirements Specification.

7. APPLICATION/INTERRELATIONSHIP (continued)

7.3 The IDD is used to document the design for those interfaces specified by an IRS, DI-MCCR-80026A. The IDD completes the description of the interface(s).

7.4 The CSCI software components that implement the interface design information required by this DID are described in a Software Design Document (SDD), DI-MCCR-80012A, for each CSCI.

7.5 This DID supersedes DI-MCCR-80027 dated 4 June 1985.

10. PREPARATION INSTRUCTIONS (continued)

- d. Document control numbers. For hardcopy formats, this document may be printed on one or both sides of each page (single-sided/double-sided). All printed pages shall contain the document control number and the date of the document centered at the top of the page. Document control numbers shall include revision and volume identification as applicable.
- e. Multiple (sub)paragraphs. All paragraphs and subparagraphs starting with the phrase "This (sub)paragraph shall..." may be written as multiple subparagraphs to enhance readability. These subparagraphs shall be numbered sequentially.
- f. Identifiers. The letters "X" and "Y" serve as identifiers for a series of descriptions. For example, the subparagraphs described by 10.1.5.2 shall be structured as follows:

3.2 (First interface name and identifier)

3.2.1 Data elements

3.2.2 Message descriptions

3.2.3 Interface priority

3.2.4 Communications protocol

3.2.4.1 (First protocol name)

3.2.4.2 (Second protocol name)

3.2.4.3 etc.

3.3 (Second interface name and identifier)

3.3.1 etc.

- g. Document structure. This specification shall consist of the following:

- (1) Cover
- (2) Title page
- (3) Table of contents
- (4) Scope
- (5) Referenced documents
- (6) Interface design
- (7) Notes
- (8) Appendixes.

10.1.1 **Title page.** The title page shall contain the information identified below in the indicated format:

[Document control number and date: Volume x of y (if multi-volume)]
 [Rev. indicator: date of Rev.]

INTERFACE DESIGN DOCUMENT

FOR THE

[SYSTEM NAME]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

Prepared for:

[Contracting Agency Name, department code]

Prepared by:

[contractor name and address]

Accepted by _____
 (Contracting agency)

Approved by _____
 Contractor

Date _____

Date _____

10.1.2 **Table of contents.** This document shall contain a table of contents listing the title and page number of each titled paragraph and subparagraph. The table of contents shall then list the title and page number of each figure, table, and appendix, in that order.

10.1.3 **Scope.** This section shall be numbered 1 and shall be divided into the following paragraphs.

10.1.3.1 **Identification.** This paragraph shall be numbered 1.1 and shall contain the approved identification number, title, and if applicable, abbreviation of the system(s), CSCI(s), and interface(s) to which this IDD applies.

10.1.3.2 System overview. This paragraph shall be numbered 1.2 and shall briefly state the purpose of the system and shall identify and describe the role of the interfaces, to which this IDD applies, within the system.

10.1.3.3 Document overview. This paragraph shall be numbered 1.3 and shall summarize the purpose and contents of this document.

10.1.4 Referenced documents. This section shall be numbered 2 and list by document and title all documents referenced in this document. This section shall also identify the source for all documents not available through normal Government stocking activities.

10.1.5 Interface Diagrams. This paragraph shall be numbered 3.1 and shall specify for each CSCI to which this IDD applies, its relationship to the other HWCI, CSCIs, or critical items with which it interfaces. This description may be provided by one or more interface diagrams, as appropriate.

10.1.5.2 (Interface name and project-unique identifier). This paragraph shall be numbered 3.X (beginning with 3.2), shall identify an interface by name and project-unique identifier, and shall state its purpose. This paragraph shall be divided into the following subparagraphs to describe the design of the interface: *This paragraph shall describe any trust-related aspects of the purpose of the interface.*

10.1.5.2.1 Data elements. This subparagraph shall be numbered 3.X.1 (beginning with 3.2.1) and shall provide, in a data element definition table, the following information, as applicable, for each data element transmitted across the interface:

- a. A project-unique identifier for the data element
- b. A brief description of the data element *including an indication of whether the data element is security-critical.*
- c. The CSCI, HWCI, or critical item that is the source of the data element
- d. The CSCI(s), HWCI(s), or critical item(s) that are the users of the data element
- e. The units of measure required for the data element, such as seconds, meters, kilohertz, etc.
- f. The limit/range of values required for the data element (for constants provide the actual value)
- g. The accuracy required for the data element
- h. The precision or resolution required for the data element in terms of significant digits
- i. The frequency at which the data element is calculated or refreshed, such as 10 KHz or 50 Msec
- j. Legality checks performed on the data element
- k. The data type, such as integer, ASCII, fixed, real, enumerated, etc.
- l. The data representation/format
- m. The priority of the data element.

10.1.5.2.2 Message descriptors. This subparagraph shall be numbered 3.X.2 (beginning with 3.2.2), shall identify each message transmitted across the interface by name and project-unique identifier, and shall describe the assignment of data elements to each message. A cross-reference of each message to the data elements that embody the message shall be provided. In addition, a cross-reference of each data element to the message(s) of which it is a part shall also be provided. Cross-references may be provided as an appendix and referenced in this subparagraph.

10.1.5.2.3 Interface priority. This subparagraph shall be numbered 3.X.3 (beginning with 3.2.3) and shall specify the relative priority of the interface and of each message transmitted across the interface.

10.1.5.2.4 Communications protocol. 10.1.5.2.4 Communications protocol. This subparagraph shall be numbered 3.X.4 (beginning with 3.2.4) and shall be divided into the following subparagraphs to describe the commercial, military, or proprietary communications protocols associated with the interface.

10.1.5.2.4.1(Protocol name). This subparagraph shall be numbered 3.X.4.Y (beginning with 3.2.4.1), shall identify a protocol by name and shall describe the technical details of the protocol. This subparagraph shall address the following communications specification details, as applicable:

- a. Fragmentation and reassembly of messages
- b. Message formatting
- c. Error control and recovery procedures, including fault tolerance features
- d. Synchronization, including connection establishment, maintenance, termination, and timing
- e. Flow control, including sequence numbering, window size, and buffer allocation
- f. Data transfer rate, whether it is periodic or aperiodic, and minimum interval between transfers
- g. Routing, addressing, and naming conventions
- h. Transmission services, including priority and grade
- i. Status, identification, notification, and any other reporting features
- j. Security, including encryption, user authentication, compartmentalization, and auditing.

10.1.6 Notes. This section shall be numbered 4 and shall contain any general information that aids in understanding this document (e.g., background information, glossary, formula derivations). This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document.

10.1.7 Appendixes. Appendixes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.), and the paragraphs within each appendix be numbered as multiples of 10 (e.g., Appendix A, paragraph 10, 10.1, 10.2, 20, 20.1, 20.2, etc.). Pages within each appendix shall be numbered alpha-numerically as follows: Appendix A pages shall be numbered A-1, A-2, A-3, etc. Appendix B pages shall be numbered B-1, B-2, B-3, etc.

DATA ITEM DESCRIPTION

SOFTWARE DEVELOPMENT PLAN

DI-MCCR-800030A-SDE

3. DESCRIPTION/PURPOSE

3.1 The Software Development Plan (SDP) describes a contractor's plans for conducting software development.

3.2 The SDP is used to provide the Government insight into the organization(s) responsible for performing software development and the methods

(continued on page 2)

380229

EC

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for that data generated under the work tasks described by paragraph 4.1.3, 4.3.3, and 4.4.1 of DOD-STD-2167A.

7.2 The Contract Data Requirements List should specify whether this document is to be prepared and delivered on bound 8 1/2 by 11 inch bond paper or electronic media. If electronic media is selected, the precise format must be specified.

(continued on page 2)

N4344

10. PREPARATION INSTRUCTIONS

10.1 Reference document. The applicable issue of the document cited herein, including its approval date and dates of any applicable amendments, notices, and revisions, shall be as specified in the contract.

10.2 Content and format instructions. Production of this plan using automated techniques is encouraged. Specific content and format instructions for this plan are identified below.

- a. Response to tailoring instructions. In the event that a paragraph or subparagraph has been tailored out, a statement to that effect shall be added directly following the heading of each such (sub)paragraph. If a paragraph and all of its subparagraphs are tailored out, only the highest level paragraph heading need be included.
- b. Use of alternate presentation styles. Charts, tables, matrices, or other presentation styles are acceptable when the information required by the paragraphs and subparagraphs of this DID can be made more readable.
- c. Page numbering. Each page prior to Section 1 shall be numbered in lower-case roman numerals beginning with page ii for the Table of Contents. Each page starting from Section 1 to the beginning of the appendixes shall be consecutively numbered in arabic numerals. If the document is divided into volumes, each such volume shall restart the page numbering sequence.

(continued on page 2)

DISTRIBUTION STATEMENT A.

Approved for public release; distribution is unlimited.

3. DESCRIPTION/PURPOSE (continued) and procedures to be followed by these organization(s).

3.3 The SDP is used by the Government to monitor the procedures, management, and contract work effort of the organizations performing software development.

7. APPLICATION/INTERRELATIONSHIP (continued)

7.3 The SDP may reference other documents (e.g., system configuration management plan) that specify the information required by this DID. The appropriate information shall be incorporated as a separate volume and delivered with the SDP.

7.4 This DID supersedes DI-MCCR-80009, DI-MCCR-80011, DI-MCCR-80030 dated 4 June 1985.

10. PREPARATION INSTRUCTIONS (continued)

d. Document control numbers. For hardcopy formats, this document may be printed on one or both sides of each page (single-sided/double-sided). All printed pages shall contain the document control number and the date of the document centered at the top of the page. Document control numbers shall include revision and volume identification as applicable.

e. Multiple (sub)paragraphs. All paragraphs and subparagraphs starting with the phrase "This (sub)paragraph shall..." may be written as multiple subparagraphs to enhance readability. These subparagraphs shall be numbered sequentially.

f. Identifiers. The letter "X" serves as an identifier for a series of descriptions. For example, the subparagraphs describing review board procedures (see 10.2.9.3.3.1) shall be structured as follows:

- 7.3.3.1 (First review board name) procedures.
- 7.3.3.2 (Second review board name) procedures.
- 7.3.3.3 etc.

g. Document structure. This plan shall consist of the following:

- (1) Cover
- (2) Title page
- (3) Table of contents
- (4) Scope
- (5) Referenced Documents
- (6) Software development management
- (7) Software engineering
- (8) Formal qualification testing
- (9) Software product evaluations
- (10) Software configuration management
- (11) Other software development functions
- (12) Notes
- (13) Appendixes.

10.2.1 Title page. The title page shall contain the information identified below in the indicated format:

[Document control number and date: Volume x of y (if multi-volume)]

[Rev. indicator: date of Rev.]

SOFTWARE DEVELOPMENT PLAN

FOR THE

[SYSTEM NAME]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

Prepared for:

[Contracting Agency Name, department code]

Prepared by:

[contractor name and address]

10.2.2 Table of contents. The software development plan shall contain a table of contents listing the title and page number of each titled paragraph and subparagraph. The table of contents shall then list the title and page number of each figure, table, and appendix, in that order.

10.2.3 Scope. This section shall be numbered 1 and shall be divided into the following paragraphs.

10.2.3.1 Identification. This paragraph shall be numbered 1.1 and shall contain the approved identification number, title, and abbreviation, if applicable, of the system to which this SDP applies. It shall also identify the CSCIs to which the plan applies. If the SDP applies to all CSCIs in the system, this shall be stated. If it applies to selected CSCIs, the applicable CSCIs shall be named by title, abbreviation, and identifier.

10.2.3.2 System overview. This paragraph shall be numbered 1.2 and shall briefly state the purpose of the system and the CSCI(s) to which this SDP applies.

10.2.3.3 Document overview. This paragraph shall be numbered 1.3 and shall summarize the purpose and contents of this document.

10.2.3.4 Relationship to other plans. This paragraph shall be numbered 1.4 and shall describe the relationship, if any, of the SDP to related project management plans. *This paragraph shall identify the Philosophy of Protection document as containing the Verification Plan required by the TCSEC (if applicable). This paragraph shall also identify the Software Test Plan document, the Software Test Description*

documents, and the Software Test Plan documents as providing the test documentation required by the TCSEC. For the TCSEC requirements for configuration management documentation, this paragraph shall identify the configuration management section of this Software Development Plan document.

10.2.4 Referenced documents. This section shall be numbered 2 and shall list by document number and title all documents referenced in this plan. This section shall also identify the source for all documents not available through normal Government stocking activities.

10.2.5 Software development management. This section shall be numbered 3 and shall be divided into the following paragraphs and subparagraphs to describe the planning associated with software development management activities.

10.2.5.1 Project organization and resources. This paragraph shall be numbered 3.1 and shall be divided into the following subparagraphs to describe the project organization and the project resources of the contractor.

10.2.5.1.1 Contractor facilities. This subparagraph shall be numbered 3.1.1 and shall provide a description of the contractor's facilities to be used for the contracted effort. This subparagraph shall highlight secure areas and briefly identify the nature of the secure activity. This subparagraph shall also highlight the location of project specific resources such as the software engineering environment and software test environment.

10.2.5.1.2 Government furnished equipment, software, and services. This subparagraph shall be numbered 3.1.2 and shall summarize all Government furnished equipment, software, services, and facilities required for the contracted effort. A schedule detailing when these items will be needed shall also be included. This subparagraph shall highlight all required items not listed in the System/Segment Specification, Prime Item Development Specification, or Critical Item Development Specification, as applicable.

10.2.5.1.3 Organizational structure. This subparagraph shall be numbered 3.1.3 and shall provide an overview of the contractor's software project organizational structure. This subparagraph shall identify the authority and responsibilities of each organization. This information may be provided graphically.

10.2.5.1.4 Personnel. This subparagraph shall be numbered 3.1.4 and shall identify the total number of personnel necessary to complete the software development project. This summary shall indicate the total number of personnel for project management, software engineering, formal software testing, software product evaluations, software configuration management and any other functions identified in this plan.

10.2.5.2 Schedule and milestones. This paragraph shall be numbered 3.2 and shall be divided into the following subparagraphs.

10.2.5.2.1 Activities. This subparagraph shall be numbered 3.2.1 and shall briefly describe each software development activity of the project and its associated schedule, based on the contract master schedule (if applicable). The development schedule shall also indicate all significant events, such as reviews, audits, key meetings, etc. The schedule may be provided graphically. For each activity, the schedule shall indicate:

- a. Activity initiation
- b. Availability of draft and final copies of formal and informal documentation
- c. Activity completion
- d. Areas of high risk.

10.2.5.2.2 Activity network. This subparagraph shall be numbered 3.2.2 and shall describe the sequential relationship among the activities of the project. This subparagraph shall include identification of those activities that impose the greatest time restrictions on project completion and those activities with an excess of time for completion. This information may be provided graphically.

10.2.5.2.3 Source Identification. This subparagraph shall be numbered 3.2.3 and shall identify and describe the source of the required resources (software, firmware, and hardware) for the software development effort. This subparagraph shall provide a plan for obtaining the required resources and shall indicate the need date and availability of each resource item.

10.2.5.3 Risk management. This paragraph shall be numbered 3.3 and shall describe the contractor's procedures for managing areas of risk to successful project completion. This paragraph shall:

- a. Identify the areas of risk to successful project completion and prioritize them.
- b. Identify the constituent risk factors that contribute to the potential occurrence of each risk.
- c. Document procedures for monitoring the risk factors and for reducing the potential occurrence of each risk.
- d. Identify contingency procedures for each area of risk, as appropriate.

10.2.5.4 Security. This paragraph shall be numbered 3.4 and shall describe the contractor's plans for implementing the security requirements of the contract *including those of the TCSEC, NCSC interpretations of the TCSEC, and/or other applicable interpreted trust requirements.*

10.2.5.5 Interface with associate contractors. This paragraph shall be numbered 3.5 and shall describe the contractor's plan for coordinating design and data management efforts to ensure compatibility at interfaces with associate contractors (i.e. where two or more contractors are participating in development or production of the system).

10.2.5.6 Interface with software IV&V agent(s). This paragraph shall be numbered 3.6 and shall describe the contractor's plans for interfacing with the software independent verification and validation (IV&V) agent(s), if applicable.

10.2.5.7 Subcontractor management. This paragraph shall be numbered 3.7 and shall describe the contractor's plans for managing subcontractors.

10.2.5.8 Formal reviews. This paragraph shall be numbered 3.8 and shall describe the contractor's internal procedures for preparing for and conducting formal reviews.

10.2.5.9 Software development library. This paragraph shall be numbered 3.9 and shall describe the software development library (SDL) to be used by the contractor for controlling the software and associated documentation. This paragraph shall include a description of the contractor's procedures and methods for establishing and implementing the SDL and the contractor's access and control procedures for data stored in the SDL.

10.2.5.10 Corrective action process. This paragraph shall be numbered 3.10 and shall describe the corrective action process to be implemented.

10.2.5.11 Problem/change report. This paragraph shall be numbered 3.11 and shall describe the format to be used for problem/change reports. These reports are used to document problems detected in the software or its documentation and to describe the corrective action needed to resolve the problems. Candidate data items for the report include:

- a. **System or project name** - The name of the system or development project to which this report applies.
- b. **Originator** - The name, telephone number, and designation of the persons or organization(s) submitting the report.
- c. **Problem number** - The assigned problem number.
- d. **Problem name** - A brief phrase descriptive of the problem and descriptive of similar problems, if applicable.
- e. **Software element or document affected** - The specific software element(s), document(s) paragraph(s), or both to which the report applies, including appropriate configuration identification and version number, if applicable.
- f. **Origination date** - The date the report is first submitted.
- g. **Category and priority** - See Appendix C of DOD-STD-2167.
- h. **Description of problem** - A description of the problem and the conditions, inputs, and equipment configuration under which the problem arises. A description of the activities leading up to problem occurrence. Sufficient problem information to permit duplication and analysis. Relationship to other reported problems and modifications.
- i. **Analyst** - The name, telephone number, and organization of the individual assigned to analyze the problem.
- j. **Date assigned** - The date the analyst was assigned.
- k. **Date complete** - The date the analysis was completed.
- l. **Analysis time** - The time required to analyze the problem.
- m. **Recommended solution** - After analysis of the problem, the recommended solution and alternative solutions, if available. The nature of the recommended solution by a short descriptive phrase. When applicable, supporting rationale and test results.
- n. **Impacts** - The cost, schedule, and interface impacts if the solution is approved. Also, performance impacts if the solution is not approved. As applicable, the impact on other systems, configuration items, other contractors, system employment, integrated logistics support, system resources, training, etc.
- o. **Problem status** - The problem status designated by configuration control procedures.
- p. **Approval of solution** - To be designated by the cognizant configuration control authority.
- q. **Follow-up action** - Actions following resolution of the problem.
- r. **Corrector** - The name, telephone number, and organization of the individual correcting the problem.
- s. **Correction date** - The date the problem was corrected.
- t. **Version number** - The version in which the problem was corrected.

u. **Correction time** - The time required to correct the problem.

v. **Implementation solution** - A brief description of the implemented solution to the problem.

10.2.6 Software engineering. This section shall be numbered 4 and shall be divided into the following paragraphs and subparagraphs to describe the planning associated with software engineering activities.

10.2.6.1 Organization and resources - software engineering. This paragraph shall be numbered 4.1 and shall be divided into the following subparagraphs to describe the organization(s) responsible and the resources necessary for software engineering activities.

10.2.6.1.1 Organizational structure - software engineering. This subparagraph shall be numbered 4.1.1 and shall describe the organization(s) responsible for performing the software engineering activities. This subparagraph shall include the authority and responsibilities of each organization and its relationship to other organizational entities such as the organization(s) responsible for performing software quality evaluations. If more than one organization is involved, the precise structure, personnel, and resources of each organization and their interrelationships shall be highlighted.

10.2.6.1.2 Personnel - software engineering. This subparagraph shall be numbered 4.1.2 and shall describe the number and skill levels of personnel who will perform the software engineering activities. The personnel shall be described by title and minimum qualifications for the position. In addition, this subparagraph shall specify any requirements unique to particular positions, such as geographic location, security level, extended hours, etc.

10.2.6.1.3 Software engineering environment. This subparagraph shall be numbered 4.1.3 and shall be divided into the following subparagraphs to identify and describe the plans for establishing and maintaining the resources (software, firmware, and hardware) necessary to perform the software engineering activities.

10.2.6.1.3.1 Software items. This subparagraph shall be numbered 4.1.3.1 and shall identify the software items, such as operating systems, compilers, code auditors, dynamic path analyzers, test drivers, preprocessors, test data generators, post-processors, etc., necessary to perform the software engineering activities. This subparagraph shall describe the purpose of each item and shall identify any classified processing or security issues associated with the software items.

10.2.6.1.3.2 Hardware and firmware items. This subparagraph shall be numbered 4.1.3.2 and shall identify the computer hardware, interfacing equipment, and firmware items that will be used in the software engineering environment. This subparagraph shall describe the purpose of each item and shall identify any classified processing or security issues associated with the hardware or firmware items.

10.2.6.1.3.3 Proprietary nature and Government rights. This subparagraph shall be numbered 4.1.3.3 and shall identify the proprietary nature and Government rights associated with each item of the software engineering environment.

10.2.6.1.3.4 Installation, control, and maintenance. This subparagraph shall be numbered 4.1.3.4 and shall identify the contractor's plans for installing and testing each item of the software engineering environment prior to its use. This subparagraph shall also describe the contractor's plans for controlling and maintaining each item of the software engineering environment.

10.2.6.2 Software standards and procedures. This paragraph shall be numbered 4.2 and shall be divided into the following subparagraphs to describe the software standards and procedures the contractor plans to use.

10.2.6.2.1 Software development techniques and methodologies. This subparagraph shall be numbered 4.2.1 and shall identify and describe the techniques and methodologies the contractor plans to use to perform:

- a. Software Requirements Analysis
- b. Preliminary Design
- c. Detailed Design
- d. Coding and CSU Testing
- e. CSC Integration and Testing
- f. CSCI Testing.

Included among these techniques shall be those required by the TCSEC (i.e. penetration testing, covert channel analysis, and verification, as applicable depending on the TCSEC level of the system). The description of these techniques shall indicate that they are required by the TCSEC.

10.2.6.2.2 Software development files. This subparagraph shall be numbered 4.2.2 and shall define the contractor's plans, including the responsible organization(s), for the creation and maintenance of software development files (SDFs). This subparagraph shall define the format and contents of the SDFs and describe the procedures for maintaining SDFs.

10.2.6.2.3 Design standards. This subparagraph shall be numbered 4.2.3 and shall describe the design standards the contractor plans to use in developing the software. *Included among these design standards shall be standards intended to meet the design requirements of the TCSEC (e.g. modularity for B2 and higher systems). The standards shall be identified as such.*

10.2.6.2.4 Coding standards. This subparagraph shall be numbered 4.2.4 and shall describe the coding standards the contractor plans to use in developing the software.

10.2.6.3 Non-developmental software. This paragraph shall be numbered 4.3 and shall identify and describe each non-developmental software item, such as commercially available, reusable, and Government furnished software, to be incorporated into the deliverable software. This subparagraph shall briefly describe the rationale for the use of each non-developmental software item.

10.2.7 Formal qualification testing. This section shall be numbered 5 and shall be divided into the following paragraphs and subparagraphs to describe the planning associated with formal qualification testing activities.

10.2.7.1 Organization and resources - formal qualification testing. This paragraph shall be numbered 5.1 and shall be divided into the following subparagraphs to describe the organization(s) responsible and the resources necessary for formal qualification testing.

10.2.7.1.1 Organizational structure - formal qualification testing. This subparagraph shall be numbered 5.1.1 and shall describe the organization(s) responsible for performing formal qualification testing. This subparagraph shall include the authority and responsibilities of each organization and its relationship to other organizational entities such as the organization(s) responsible for performing software engineering. If more than one organization is involved, the precise structure, personnel, and resources of each organization and their interrelationships shall be highlighted.

10.2.7.1.2 Personnel - formal qualification testing. This subparagraph shall be numbered 5.1.2 and shall describe the number and skill levels of personnel who will perform the formal qualification testing activities. The personnel shall be described by title and minimum qualifications for the position. In addition, this subparagraph shall specify any requirements unique to particular positions, such as geographic location, security level, extended hours, etc.

10.2.7.2 Test approach/philosophy. This paragraph shall be numbered 5.2 and shall describe the contractor's approach/philosophy for performing formal qualification testing.

10.2.7.3 Test planning assumptions and constraints. This paragraph shall be numbered 5.3 and shall describe any assumptions that were made in test planning and any constraints imposed upon formal qualification testing by the contracting agency.

10.2.8 Software product evaluations. This section shall be numbered 6 and shall be divided into the following paragraphs and subparagraphs to describe the planning associated with software product evaluation activities.

10.2.8.1 Organization and resources - software product evaluations. This paragraph shall be numbered 6.1 and shall be divided into the following subparagraphs to describe the organization(s) responsible and the resources necessary for software product evaluations.

10.2.8.1.1 Organizational structure - software product evaluations. This subparagraph shall be numbered 6.1.1 and shall describe the organization(s) responsible for performing the software product evaluations. This subparagraph shall include the authority and responsibilities of each organization and its relationship to other organizational entities such as the organization(s) responsible for performing software engineering. If more than one organization is involved, the precise structure, personnel, and resources of each organization and their interrelationships shall be highlighted.

10.2.8.1.2 Personnel - software product evaluations. This subparagraph shall be numbered 6.1.2 and shall describe the number and skill levels of personnel who will perform software product evaluations. The personnel shall be described by title and minimum qualifications for the position. In addition, this subparagraph shall specify any requirements unique to particular positions, such as geographic location, security level, extended hours, etc. *The personnel described shall include personnel for any relevant TCSEC-required evaluation method (e.g. penetration testing, covert channel analysis, depending on the TCSEC level of the system). These evaluation methods shall be identified as being required by the TCSEC.*

10.2.8.2 Software product evaluations procedures and tools. This paragraph shall be numbered 6.2 and shall be divided into the following subparagraphs.

10.2.8.2.1 Procedures. This subparagraph shall be numbered 6.2.1 and shall identify and describe the procedures that will be used to evaluate the software and associated documentation.

10.2.8.2.2 Tools. This subparagraph shall be numbered 6.2.2 and shall identify and describe the tools to be used in the software product evaluations. Tool descriptions shall identify each tool's purpose in the evaluation process. To reduce duplication, references may be made to tools that are also used in the software engineering or software test environments.

10.2.8.3 Subcontractor products. This paragraph shall be numbered 6.3 and shall describe the contractor's plans and procedures for evaluating the adequacy of requirements established for subcontractors and for evaluating subcontractor products.

10.2.8.4 Software product evaluation records. This paragraph shall be numbered 6.4 and shall describe the contractor's plans for preparing and maintaining records of each product evaluation performed. It shall identify the formats to be used and the information to be recorded for each evaluation. It shall also describe plans for maintaining the records and for making them available for contracting agency review.

10.2.8.5 Activity-dependent product evaluations. This paragraph shall be numbered 6.5 and shall be divided into subparagraphs to describe the contractor's plans for conducting product evaluations of each software development product. This subparagraph shall explain any planned modifications or additions to the evaluation criteria required by DOD-STD-2167. The following subparagraphs shall address plans for product evaluations conducted during each of the software development activities (i.e., System Requirements Analysis/Design, Software Requirements Analysis, Preliminary Design, Detailed Design, Coding and CSU Testing, CSC Integration and Testing, CSCI Testing, and System Integration and Testing).

10.2.8.5.1 Software products evaluation - (activity name). This subparagraph shall be numbered 6.5.X (beginning with 6.5.1) and shall describe the contractor's plans for conducting evaluations of each of the products of an activity. The description shall identify the specific products to be evaluated. For each product to be evaluated, the evaluation criteria to be used and the evaluation procedures and tools to be employed shall be identified. For evaluations performed on items contained in SDFs, the method selecting the sample and the percentage of the items to be evaluated shall be specified.

10.2.9 Software configuration management. This section shall be numbered 7 and shall be divided into the following paragraphs and subparagraphs to describe the planning associated with software configuration management (CM) activities.

10.2.9.1 Organization and resources - configuration management. This paragraph shall be numbered 7.1 and shall be divided into the following subparagraphs to describe the organization(s) responsible and the resources necessary for configuration management.

10.2.9.1.1 Organizational structure - configuration management. This subparagraph shall be numbered 7.1.1 and shall describe the organization(s) responsible for performing configuration management. This subparagraph shall include the authority and responsibilities of each organization and its relationship to other organizational entities such as the organization(s) responsible for performing software engineering. If more than one organization is involved, the precise structure, personnel, and resources of each organization and their interrelationships shall be highlighted.

10.2.9.1.2 Personnel - configuration management. This subparagraph shall be numbered 7.1.2 and shall describe the number and skill levels of personnel who will perform configuration management. The personnel shall be described by title and minimum qualifications for the position. In addition, this subparagraph shall specify any requirements unique to particular positions, such as geographic location, security level, extended hours, etc.

10.2.9.2 Configuration identification. This paragraph shall be numbered 7.2 and shall be divided into the following subparagraphs.

10.2.9.2.1 Developmental configuration identification. This subparagraph shall be numbered 7.2.1 and shall identify the contractor's internal Developmental Configuration(s) to be used in the development of the CSCI(s). For each Developmental Configuration identified, the method of establishing it shall be described and the contents shall be listed.

10.2.9.2.2 Identification methods. This subparagraph shall be numbered 7.2.2 and shall describe the methods to be used in identifying (e.g., naming, marking, numbering) CSCI(s), CSCs, CSUs, and documentation. This subparagraph shall also describe how revisions to the CSCI(s), CSCs, CSUs, and documentation shall be identified.

10.2.9.3 Configuration control. This paragraph shall be numbered 7.3 and shall be divided into the following subparagraphs to provide a detailed description of the procedures to be used in controlling changes to and maintaining the Developmental Configuration(s) and internally controlled documentation.

10.2.9.3.1 Flow of configuration control. This subparagraph shall be numbered 7.3.1 and shall describe the process by which problems and changes are submitted, reviewed, and subsequently approved or disapproved. This description may be accomplished graphically by a configuration control flow chart (see Figure 1).

10.2.9.3.2 Reporting documentation. This subparagraph shall be numbered 7.3.2 and shall be divided into the following subparagraphs to describe or reference the description of the reporting documentation, such as Specification Change Notices and Engineering Change Proposals, to be used in controlling software problems and changes.

10.2.9.3.2.1 (Report name). This subparagraph shall be numbered 7.3.2.X (beginning with 7.3.2.1) and shall describe or reference the format, contents, and instructions for completing the report.

10.2.9.3.3 Review procedures. This subparagraph shall be numbered 7.3.3 and shall be divided into the following subparagraphs to describe the purpose of, and the procedures to be employed by, any review boards associated with the flow of configuration control.

10.2.9.3.3.1 (Review board name) procedures. This subparagraph shall be numbered 7.3.3.X (beginning with 7.3.3.1) and shall describe the purpose of and the procedures to be followed by the review board. This subparagraph shall also describe how the procedures used by the review board, in conjunction with the configuration identification scheme, provide historical traceability.

10.2.9.3.4 Storage, handling, and delivery of project media. This subparagraph shall be numbered 7.3.4 and shall describe the methods and procedures to be used to formally control the storage, handling, and delivery of deliverable software and documentation (including master copies) during the development process.

10.2.9.3.5 Additional control. This subparagraph shall be numbered 7.3.5 and shall identify any additional configuration control activities not discussed above.

10.2.9.4 Configuration status accounting. This paragraph shall be numbered 7.4 and shall define the configuration status accounting system to be used. The content, format, and purpose of the status accounting records and reports shall be described.

10.2.9.5 Configuration audits. This paragraph shall be numbered 7.5 and shall describe the contractor's plans for supporting or conducting configuration audits, as applicable. The description of how the configuration status accounting reports and records should be used in conducting these audits shall be included.

10.2.9.6 Preparation for specification authentication. This paragraph shall be numbered 7.6 and shall describe the contractor's procedures to prepare for and respond to authentication of the applicable specifications. This paragraph shall include the procedures for:

FIGURE 1. Example of a configuration control flow chart.

- a. Submitting specifications to the contracting agency for review and authentication.
- b. Ensuring the incorporation of approved changes.
- c. Updating the configuration status accounting reports to reflect approved baseline(s).

10.2.9.7 Configuration management major milestones. This paragraph shall be numbered 7.7 and shall identify the major internal and Government milestones related to software configuration management for the contractual effort.

10.2.10 Other software development functions. This section shall be numbered 8 and shall be divided into the following paragraphs and subparagraphs to describe any other contractor functions involved in the software development effort. *Included among these other functions shall be those required by the TCSEC: modeling, formal analysis, verification, covert channel analysis, and penetration testing (depending on the TCSEC level of the system). These techniques shall be identified as being required by the TCSEC.*

10.2.10.1 (Function name). This paragraph shall be numbered 8.X (beginning with 8.1) and shall describe a function to be performed. This paragraph shall be divided into the following subparagraphs to describe the organizational structure, resources, and the methods and procedures necessary to perform the function.

10.2.10.1.1 Organizational structure - (function name). This subparagraph shall be numbered 8.X.1 (beginning with 8.1.1) and shall describe the organization(s) responsible for performing the function. This subparagraph shall include the authority and responsibilities of each organization and its relationship to other organizational entities such as the organization(s) responsible for performing configuration management. If more than one organization is involved, the precise structure, personnel, and resources of each organization and their interrelationships shall be highlighted.

10.2.10.1.2 Personnel - (function name). This subparagraph shall be numbered 8.X.2 and shall describe the number and skill levels of personnel who will perform the function. The personnel shall be described by title and minimum qualifications for the position. In addition, this subparagraph shall specify any requirements unique to particular positions, such as geographic location, security level, extended hours, etc.

10.2.10.1.3 Other resources - (function name). This subparagraph shall be numbered 8.X.3 and shall identify and describe any other resources necessary for performing the function. For each resource, this subparagraph shall briefly describe the aspect of the function that requires the resource.

10.2.10.1.4 Methods and procedures - (function name). This subparagraph shall be numbered 8.X.4 and shall describe the methods and procedures to be used to perform the function.

10.2.11 Notes. This section shall be numbered 9 and shall contain any general information that aids in understanding this document. This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document.

10.2.12 Appendixes. Appendixes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.), and the paragraphs within each appendix be numbered as multiples of 10 (e.g., Appendix

A, paragraph 10, 10.1, 10.2, 20, 20.1, 20.2, etc.). Pages within each appendix shall be numbered alpha-numerically as follows: Appendix A pages shall be numbered A-1, A-2, A-3, etc. Appendix B pages shall be numbered B-1, B-2, B-3, etc.

DATA ITEM DESCRIPTION

COMPUTER SYSTEM OPERATOR'S MANUAL

DI-MCCR-80018A-SDE

3. DESCRIPTION/PURPOSE

3.1 The Computer System Operator's Manual (CSOM) provides information and detailed procedures for initiating, operating, monitoring, and shutting down a computer system and for identifying/isolating a malfunctioning component in a computer system.

3.2 A CSOM is developed for each computer system in which one or more CSCIs execute.

(continued on page 2)

380229

EC

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for data generated under the work task described by paragraph 4.6.4 of DOD STD-2167A.

7.2 The Contract Data Requirements List should specify whether this document is to be prepared and delivered on bound 8 1/2 by 11 inch bond paper or electronic media. If electronic media is selected, the precise format must be specified.

(continued on page 2)

N4335

10. PREPARATION INSTRUCTIONS

10.1 Content and format instructions Production of this manual using automated techniques is encouraged. Specific content and format instructions for this manual are identified below.

- a. Response to tailoring instructions. In the event that a paragraph or subparagraph has been tailored out, a statement to that effect shall be added directly following the heading of each such (sub)paragraph. If a paragraph and all of its subparagraphs are tailored out, only the highest level paragraph heading need be included.
- b. Use of alternate presentation styles. Charts, tables, matrices, or other presentation styles are acceptable when the information required by the paragraphs and subparagraphs of this DID can be made more readable.
- c. Page numbering. Each page prior to Section 1 shall be numbered in lower-case roman numerals beginning with page ii for the Table of Contents. Each page starting from Section 1 to the beginning of the appendixes shall be consecutively numbered in arabic numerals. If the document is divided into volumes, each such volume shall restart the page numbering sequence.

(continued on page 2)

DISTRIBUTION STATEMENT A.

Approved for public release; distribution is unlimited.

7. APPLICATION/INTERRELATIONSHIP (continued)

7.3 This DID supersedes DI MCCR-80018 and DI MCCR-80020 dated 4 June 1985.

10. PREPARATION INSTRUCTIONS (continued)

- d. Document control numbers. For hardcopy formats, this document may be printed on one or both sides of each page (single sided/double sided). All printed pages shall contain the document control number and the date of the document centered at the top of the page. Document control numbers shall include revision and volume identification as applicable.
- e. Multiple (sub)paragraphs. All paragraphs and subparagraphs starting with the phrase "This (sub)paragraph shall..." may be written as multiple subparagraphs to enhance readability. These subparagraphs shall be numbered sequentially.
- f. Identifiers. The letter "X" serves as an identifier for a series of descriptions. For example, the subparagraphs of paragraph 10.1.6.2 describes diagnostic procedures and is presented in the following structure:

4.2 Diagnostic procedures.

4.2.1 (Name of the first diagnostic procedure).

4.2.2 (Name of the second diagnostic procedure).

4.2.3 etc.

- g. Document structure. This manual shall consist of the following:

- (1) Cover
- (2) Title page
- (3) Table of contents
- (4) Scope
- (5) Referenced Documents
- (6) Computer system operation
- (7) Diagnostic features
- (8) Notes
- (9) Appendixes.

10.2.1 **Title page.** The title page shall contain the information identified below in the indicated format:

[Document control number and date: Volume x of y (if multi-volume)]

[Rev. indicator: date of Rev.]

COMPUTER SYSTEM OPERATOR'S MANUAL

FOR THE

[SYSTEM NAME]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

Prepared for:

[Contracting Agency Name, department code]

Prepared by:

[contractor name and address]

10.1.2 Table of contents. This manual shall contain a table of contents listing the title and page number of each titled paragraph and subparagraph. The table of contents shall then list the title and page number of each figure, table, and appendix, in that order.

10.1.3 Scope. This section shall be numbered 1 and shall be divided into the following paragraphs.

10.1.3.1 Identification. This paragraph shall be numbered 1.1 and shall contain the approved identification number, title, and abbreviation, if applicable, of the computer system to which this CSOM applies.

10.1.3.2 System overview. This paragraph shall be numbered 1.2 and shall briefly state the purpose of the system and the software to which this CSOM applies.

10.1.3.3 Document overview. This paragraph shall be numbered 1.3 and shall summarize the purpose and contents of this manual.

10.1.4 Referenced documents. This section shall be numbered 2 and shall list by document number and title all documents referenced in this manual. This section shall also identify the source for all documents not available through normal Government stocking activities.

10.1.5 Computer system operation. This section shall be numbered 3 and shall be divided into the following paragraphs and subparagraphs to describe the instructions for operation of the computer system. This section may reference commercially available documents for the information required by the following paragraphs and subparagraphs. *This section shall describe the operational and administrative functionality related to security (including cautions about functions and privileges that should be controlled when operating the trusted system), and shall provide any other information required by the TCSEC Trusted Facility Manual requirements for the TCSEC level and/or interpretations.*

10.1.5.1 Computer system preparation and shutdown. This paragraph shall be numbered 3.1 and shall be divided into the following subparagraphs to describe the procedures for computer system preparation and setup prior to computer system operation.

10.1.5.1.1 Power on and off. This subparagraph shall be numbered 3.1.1 and shall explain the step by step procedures required to power on and power off the computer system.

10.1.5.1.2 Initiation. This subparagraph shall be numbered 3.1.2 and shall contain the initiation procedures necessary to operate the computer system. This subparagraph shall describe the following:

- a. The equipment setup and the procedures required for pre operation.
- b. The procedures necessary to bootstrap the computer system and to load software and data.
- c. The commands typically used during computer system initiation.
- d. The procedures necessary to initialize files, variables, or other parameters.

10.1.5.1.3 Shutdown. This subparagraph shall be numbered 3.1.3 and shall contain the shutdown procedures necessary to save data files and other information and to terminate computer system operation.

10.1.5.2 Operating procedures. This paragraph shall be numbered 3.2 and shall be divided into the following subparagraphs to contain the procedures necessary to operate the computer system once the initiation procedures are complete. If more than one mode of operation is available, instructions for each mode shall be provided.

10.1.5.2.1 Input and output procedures. This subparagraph shall be numbered 3.2.1, shall describe the input and output media (e.g., magnetic tape, disk, cartridge, etc.) relevant to the computer system and shall explain the procedures required to read and write on these media. This subparagraph shall briefly describe the operating system control language and shall also list operator procedures for interactive messages and replies (e.g., which terminal to use, password use, log on and log off procedures).

10.1.5.2.2 Monitoring procedures. This subparagraph shall be numbered 3.2.2 and shall contain the procedures to be followed for monitoring the software in operation. Applicable trouble and malfunction indications shall be included. Evaluation techniques for fault isolation shall be described to the maximum extent practical. This subparagraph shall also include descriptions of conditions requiring computer system shutdown. Procedures for on-line intervention, abort, and user communications shall also be included.

10.1.5.2.3 Recovery procedures. This subparagraph shall be numbered 3.2.3 and shall describe the automatic and manual procedures to be followed for each trouble occurrence (e.g., give detailed instructions to obtain computer system dumps). This subparagraph shall describe the steps to be taken by the operator to restart computer system operation after an abort or interruption of operation. Procedures for recording information concerning a malfunction shall also be included.

10.1.5.2.4 Off-line routine procedures. This subparagraph shall be numbered 3.2.4 and shall contain the procedures required to operate all relevant off-line routines of the computer system.

10.1.5.2.5 Other procedures. This subparagraph shall be numbered 3.2.5 and shall contain any additional procedures to be followed by the operator (e.g., computer system alarms, program or computer system security considerations, switch over to a redundant computer system).

10.1.6 Diagnostic features. This section shall be numbered 4 and shall be divided into the following paragraphs and subparagraphs to describe the diagnostic features available to the computer operator. This section may reference commercially available documents for the information required by the following paragraphs and subparagraphs.

10.1.6.1 Diagnostic features summary. This paragraph shall be numbered 4.1 and shall summarize the error detection and diagnostic features available in the computer system, including error message syntax and hierarchy for fault isolation. This paragraph shall describe the purpose of each diagnostic feature.

10.1.6.2 Diagnostic procedures. This paragraph shall be numbered 4.2 and shall be divided into the following subparagraphs to identify and describe the diagnostic procedures.

10.1.6.2.1 (Procedure name). This subparagraph shall be numbered 4.2.X (beginning with 4.2.1), shall identify a diagnostic procedure, and shall describe its purpose. Reference may be made to section 3 of this document, as appropriate, for computer system operating instructions that support the diagnostic procedure. This subparagraph shall describe:

- a. Hardware, software, or firmware necessary for executing the procedure
- b. Step by step instructions for executing the procedure
- c. Diagnostic messages and the corresponding required action.

10.1.6.3 Diagnostic tools. This paragraph shall be numbered 4.3 and shall be divided into the following subparagraphs to describe each diagnostic tool available to the computer operator. A diagnostic tool may contain hardware, software, firmware, or a combination of these and provides diagnostic capabilities.

10.1.6.3.1 (Diagnostic tool name). This subparagraph shall be numbered 4.3.X (beginning with 4.3), shall identify a diagnostic tool by name and number and shall describe the tool and its application.

10.1.7 Notes. This section shall be numbered 6 and shall contain any general information that aids in understanding this document (e.g., background information, glossary). This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document.

10.1.8 Appendixes. Appendixes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.), and the paragraphs within each appendix be numbered as multiples of 10 (e.g., Appendix A, paragraph 10, 10.1, 10.2, 20, 20.1, 20.2, etc.). Pages within each appendix shall be numbered alpha numerically as follows: Appendix A pages shall be numbered A-1, A-2, A-3, etc. Appendix B pages shall be numbered B-1, B-2, B-3, etc.

DATA ITEM DESCRIPTION

SOFTWARE USER'S MANUAL

DI-MCCR-80019A-SDE

3. DESCRIPTION/PURPOSE

3.1 The Software User's Manual (SUM) provides user personnel with instructions sufficient to execute one or more related Computer Software Configuration Items (CSCIs).

3.2 The SUM provides the steps for executing the software, the expected output, and the measures to be taken if error messages appear.

(continued on page 2)

380229

EC

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for data generated under the work task described by paragraph 4.6.4 of DOD-STD-2167A.

7.2 The Contract Data Requirements List should specify whether this document is to be prepared and delivered on bound 8 1/2 by 11 inch bond paper or electronic media. If electronic media is selected, the precise format must be specified.

(continued on page 2)

N4336

10. PREPARATION INSTRUCTIONS

10.1 Content and format instructions. Production of this manual using automated techniques is encouraged. Specific content and format instructions for this manual are identified below.

- a. Response to tailoring instructions. In the event that a paragraph or subparagraph has been tailored out, a statement to that effect shall be added directly following the heading of each such (sub)paragraph. If a paragraph and all of its subparagraphs are tailored out, only the highest level paragraph heading need be included.
- b. Use of alternate presentation styles. Charts, tables, matrices, or other presentation styles are acceptable when the information required by the paragraphs and subparagraphs of this DID can be made more readable.
- c. Page numbering. Each page prior to Section 1 shall be numbered in lower-case roman numerals beginning with page ii for the Table of Contents. Each page starting from Section 1 to the beginning of the appendixes shall be consecutively numbered in arabic numerals. If the document is divided into volumes, each such volume shall restart the page numbering sequence.

(continued on page 2)

DISTRIBUTION STATEMENT A.

Approved for public release; distribution is unlimited.

3. DESCRIPTION PURPOSE (continued)

3.3 The information required by this DID is directed to the functional user of the CSCI(s), as opposed to the operator of the computer system. If this distinction does not exist, the user will need to refer to both the Computer System Operator's Manual and the SUM to operate the computer system and to use the CSCI(s)

7. APPLICATION/INTERRELATIONSHIP (continued)

7.4 This DID supersedes DI-MCCR-80019 dated 4 June 1985.

10. PREPARATION INSTRUCTIONS (continued)

- d. Document control numbers. For hardcopy formats, this document may be printed on one or both sides of each page (single-sided/double-sided). All printed pages shall contain the document control number and the date of the document centered at the top of the page. Document control numbers shall include revision and volume identification, as applicable.
- e. Multiple (sub)paragraphs. All paragraphs and subparagraphs starting with the phrase "This (sub)paragraph shall..." may be written as multiple subparagraphs to enhance readability. These subparagraphs shall be numbered sequentially.
- f. Document structure. This manual shall consist of the following:
 - (1) Cover
 - (2) Title page
 - (3) Table of contents
 - (4) Scope
 - (5) Referenced documents
 - (6) Execution procedures
 - (7) Error messages
 - (8) Notes
 - (9) Appendixes.

10.1.1 **Title page.** The title page shall contain the information identified below in the indicated format:

[Document control number and date: Volume x of y (if multi-volume)]

[Rev. indicator: date of Rev.]

SOFTWARE USER'S MANUAL

FOR THE

[SYSTEM NAME]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

Prepared for:

[Contracting Agency Name, department code]

Prepared by:

[contractor name and address]

10.1.2 Table of contents. This manual shall contain a table of contents listing the title and page number of each titled paragraph and subparagraph. The table of contents shall then list the title and page number of each figure, table, and appendix, in that order.

10.1.3 Scope. This section shall be numbered 1 and shall be divided into the following paragraphs.

10.1.3.1 Identification. This paragraph shall be numbered 1.1 and shall contain the approved identification number(s), version number, release number, title(s), and abbreviation(s), if applicable, of the CSCI(s) and the system to which this SUM applies.

10.1.3.2 System overview. This paragraph shall be numbered 1.2 and shall briefly state the purpose of the system and the CSCI(s) to which this SUM applies.

10.1.3.3 Document overview. This paragraph shall be numbered 1.3 and shall summarize the purpose and contents of this manual.

10.1.4 Referenced documents. This section shall be numbered 2 and shall list by document number and title all documents referenced in this manual. This section shall also identify the source for all documents not available through normal Government stocking activities.

10.1.5 Execution procedures. This section shall be numbered 3 and shall present the information and instructions necessary for user interaction with the CSCI(s) in order to carry out the operation of the software. *This section shall describe the protection mechanism provided by the TCB, guidelines on their use, and how they interact with one another.* This subparagraph shall describe the step-by-step procedures for executing the software and shall identify the options available to the user. Reference may be made to an operator's manual for the computer system operating procedures (e.g. Computer System Operator's Manual (CSOM), DI-MCCR- 30018). The procedures shall include the following information as applicable:

- a. Initialization. Describe the initialization procedures necessary to execute the software. Identify any initialization options available to the user.
- b. User inputs. Describe the user inputs to the software.

- c. System inputs. Describe the system inputs to the software that may occur while the software is in use and that may affect the software's interface with the user (e.g., inputs from a remote sensor). Include format, frequency, allowable range, and units of measure, as applicable.
- d. Termination. Describe how to terminate software operation and how the user can determine whether normal termination has occurred.
- e. Restart. Describe the procedures for restarting the software.
- f. Outputs. Describe expected outputs of the software, including error messages.

10.1.6 Error messages. This section shall be numbered 4 and shall identify all error messages output by the software, the meaning of each error message, and the action to be taken when each message appears.

10.1.7 Notes. This section shall be numbered 5 and shall contain any general information that aids in understanding this document (e.g., background information, glossary). This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings used in this document.

10.1.8 Appendixes. Appendixes may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.), and the paragraphs within each appendix be numbered as multiples of 10 (e.g., Appendix A, paragraph 10, 10.1, 10.2, 20, 20.1, 20.2, etc.). Pages within each appendix shall be numbered alpha-numerically as follows: Appendix A pages shall be numbered A-1, A-2, A-3, etc. Appendix B pages shall be numbered B-1, B-2, B-3, etc.

5 Tools

5.1 Paragraph Report

The following pages present a report of tailoring by DID and paragraph number. The annotation, "Additional Security Requirements Apply" is meant to indicate that the tailoring guidance presented in the Section 2 should be used to complete the DID.

TAILOR/DIDs-2167A
 DETAILED REPLACE REPORT
 PROJECT: SDE
 DATE: 5/27/92
 TIME: 22:42

Computer System Operator's Manual (CSOM)

Paragraph	Title/Subject	Status			
		K	D	R	T
10.1.5	Computer system operation CDRL will say: Additional Security Requirements apply.			R	

DETAILED REPLACE REPORT for SDE, 5/27/92, 22:42 (page 2)

Interface Design Document (IDD)

Paragraph	Title/Subject	Status			
		K	D	R	T
10.1.5.2	(Interface name and project-unique identifier) CDRL will say: Additional Security Requirements Apply			R	
10.1.5.2.2	Message descriptions CDRL will say: Additional Security Requirements Apply			R	

DETAILED REPLACE REPORT for SDE, 5/27/92, 22:42 (page 3)

Interface Requirements Specification (IRS)

Paragraph	Title/Subject	Status
		K D R T
10.1.5.2	(Interface name and project-unique identifier) CDRL will say: Additional Security Requirements Apply	R
10.1.5.2.2	Data requirements CDRL will say: Additional Security Requirements Apply	R

DETAILED REPLACE REPORT for SDE, 5/27/92, 22:42 (page 4)

Software Design Document (SDD)

Paragraph	Title/Subject	Status
		K D R T
10.1.5.1	CSCI overview CDRL will say: Additional Security Requirements Apply	R
10.1.5.1.1	CSCI architecture CDRL will say: Additional Security Requirements Apply	R
10.1.5.2.1	(CSC name and project-unique identifier) CDRL will say: Additional Security Requirements Apply	R
10.1.5.2.1.a	(Requirements allocated to the CSC) CDRL will say: Additional Security Requirements Apply	R
10.1.5.2.1.b	(Execution control and data flow) CDRL will say: Additional Security Requirements Apply	R
10.1.5.2.1.c	(Design requirements)	R

	CDRL will say: Additional Security Requirements Apply	
10.1.6.1	(CSC name and project-unique identifier) CDRL will say: Additional Security Requirements Apply	R
10.1.6.1.2	(CSU name and project-unique identifier) CDRL will say: Additional Security Requirements Apply	R
10.1.6.1.2.1	(CSU name) Design specification/constraints CDRL will say: Additional Security Requirements Apply	R
10.1.6.1.2.2	(CSU name) Design CDRL will say: Additional Security Requirements Apply	R
10.1.7	CSCI data CDRL will say: Additional Security Requirements Apply	R
10.1.8	CSCI data files CDRL will say: Additional Security Requirements Apply	R

DETAILED REPLACE REPORT for SDE, 5/27/92, 22:42 (page 5)

Software Design Document (continued)

Paragraph	Title/Subject	Status K D R T
10.1.11	Appendixes CDRL will say: Additional Security Requirements Apply	R

DETAILED REPLACE REPORT for SDE, 5/27/92, 22:42 (page 6)

Software Development Plan (SDP)

Paragraph	Title/Subject	Status			
		K	D	R	T
10.2.3.4	Relationship to other plans CDRL will say: Additional Security Requirements Apply			R	
10.2.5.4	Security CDRL will say: Additional Security Requirements Apply			R	
10.2.6.2.1	S/W development techniques and methodologies CDRL will say: Additional Security Requirements Apply			R	
10.2.6.2.3	Design standards CDRL will say: Additional Security Requirements Apply			R	
10.2.8.1.2	Personnel - software product evaluations CDRL will say: Additional Security Requirements Apply			R	
10.2.10	Other software development functions CDRL will say: Additional Security Requirements Apply			R	

DETAILED REPLACE REPORT for SDE, 5/27/92, 22:42 (page 7)

Software Requirements Specification (SRS)

Paragraph	Title/Subject	Status			
		K	D	R	T

10.1.5	Engineering requirements CDRL will say: Delete reference to PIDS and CIDS.	R
10.1.5.1	CSCI external interface requirements CDRL will say: Additional Security Requirements Apply	R
10.1.5.8	Security requirements CDRL will say: Additional Security Requirements Apply	R
10.1.5.9	Design constraints CDRL will say: Additional Security Requirements Apply	R
10.1.5.10	Software quality factors CDRL will say: Additional Security Requirements Apply	R
10.1.5.12	Requirements traceability CDRL will say: Delete references to PIDS and CIDS. Additional Security	R
10.1.6.1	Qualification methods CDRL will say: Additional Security Requirements Apply	R

DETAILED REPLACE REPORT for SDE, 5/27/92, 22:42 (page 8)

System/Segment Design Document (SSDD)

Paragraph	Title/Subject	Status			
		K	D	R	T
10.1.3.2	System overview CDRL will say: Additional Security Requirements Apply			R	

10.1.5.4	System architecture CDRL will say: Additional Security Requirements Apply	R
10.1.6.1.1	(HWCi name and project-unique identifier) CDRL will say: Additional Security Requirements Apply	R
10.1.6.2.1	(CSCI name and project-unique identifier) CDRL will say: Additional Security Requirements Apply	R

DETAILED REPLACE REPORT for SDE, 5/27/92, 22:42 (page 9)

Software User's Manual (SUM)

Paragraph	Title/Subject	Status
		K D R T
10.1.5	Execution procedures CDRL will say: Additional Security Requirements Apply	R

5.2 Report Outlines

The following pages present an outline for each of the required documents. The annotation, "Additional Security Requirements Apply" is meant to indicate that the tailoring guidance presented in the Section 2 should be used to complete the DID.

TAILOR/DIDs-2167A
DOCUMENT OUTLINE REPORT
PROJECT: SDE
DATE: 5/27/92
TIME: 22:38

Computer System Operator's Manual (CSOM)

1. Scope
 - 1.1 Identification
 - 1.2 System overview
 - 1.3 Document overview
2. Referenced documents
3. Computer system operation
(Additional Security Requirements apply.)
 - 3.1 Computer system preparation and shutdown
 - 3.1.1 Power on and off
 - 3.1.2 Initiation
 - 3.1.2.a (Equipment setup and pre-operation procedures)
 - 3.1.2.b (Bootstrap and loading procedures)
 - 3.1.2.c (Initiation commands)
 - 3.1.2.d (Data initialization procedures)
 - 3.1.3 Shutdown

3.2 Operating procedures

3.2.1 Input and output procedures

3.2.2 Monitoring procedures

3.2.3 Recovery procedures

3.2.4 Off-line routine procedures

3.2.5 Other procedures

4. Diagnostic features

4.1 Diagnostic features summary

4.2 Diagnostic procedures

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 2)

Computer System Operator's Manual (continued)

4.2.1 (Procedure name)

4.2.1.a (Required hardware, software, firmware)

4.2.1.b (Instructions for executing the procedure)

4.2.1.c (Diagnostic messages and required actions)

4.3 Diagnostic tools

4.3.1 (Diagnostic tool name)

6. Notes

(Appendixes)

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 3)

Interface Design Document (IDD)

1. Scope

1.1 Identification

1.2 System overview

1.3 Document overview

2. Referenced documents

3. Interface design

3.1 Interface diagrams

3.2 (Interface name and project-unique identifier)
(Additional Security Requirements Apply)

3.2.1 Data elements

3.2.1.a (Data element identifier)

3.2.1.b (Data element description)

3.2.1.c (Source)

3.2.1.d (Destination)

3.2.1.e (Units)

3.2.1.f (Limit/range)

3.2.1.g (Accuracy)

3.2.1.h (Precision)

- 3.2.1.i (Frequency)
- 3.2.1.j (Legality checks)
- 3.2.1.k (Data type)
 - 3.2.1.1 (Data representation/format)
 - 3.2.1.m (Priority)
- 3.2.2 Message descriptions
(Additional Security Requirements Apply)
- 3.2.3 Interface priority
- 3.2.4 Communications protocol

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 4)

Interface Design Document (continued)

-
- 3.2.4.1 (Protocol name)
 - 3.2.4.1.a (Fragmentation/reassembly of messages)
 - 3.2.4.1.b (Message formatting)
 - 3.2.4.1.c (Error control/recovery)
 - 3.2.4.1.d (Synchronization)
 - 3.2.4.1.e (Flow control)
 - 3.2.4.1.f (Data transfer rate)
 - 3.2.4.1.g (Routing, addressing, naming conventions)

3.2.4.1.h (Transmission services)

3.2.4.1.i (Reporting features)

3.2.4.1.j (Security)

4. Notes

(Appendixes)

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 5)

Interface Requirements Specification (IRS)

1. Scope

1.1 Identification

1.2 System overview

1.3 Document overview

2. Applicable documents

2.1 Government documents

2.2 Non-Government documents

3. Interface specification

3.1 Interface diagrams

3.2 (Interface name and project-unique identifier)
(Additional Security Requirements Apply)

3.2.1 Interface requirements

3.2.1.a (Concurrent vs sequential execution)

3.2.1.b (Communication protocol)

3.2.1.c (Priority level of the interface)

3.2.2 Data requirements
(Additional Security Requirements Apply)

3.2.2.a (Data element identifier)

3.2.2.b (Data element description)

3.2.2.c (Source)

3.2.2.d (Destination)

3.2.2.e (Units)

3.2.2.f (Limit/range)

3.2.2.g (Accuracy)

3.2.2.h (Precision)

4. Quality Assurance

5. Preparation for delivery

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 6)

Interface Requirements Specification (continued)

6. Notes

(Appendixes)

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 7)

Software Design Document (SDD)

1. Scope

1.1 Identification

1.2 System overview

1.3 Document overview

2. Referenced documents

3. Preliminary design

3.1 CSCI overview

(Additional Security Requirements Apply)

3.1.1 CSCI architecture

(Additional Security Requirements Apply)

3.1.2 System states and modes

3.1.3 Memory and processing time allocation

3.2 CSCI design description

3.2.1 (CSC name and project-unique identifier)

(Additional Security Requirements Apply)

3.2.1.a (Requirements allocated to the CSC)

(Additional Security Requirements Apply)

3.2.1.b (Execution control and data flow)

(Additional Security Requirements Apply)

3.2.1.c (Design requirements)

(Additional Security Requirements Apply)

3.2.1.1 (Sub-level CSC name and identifier)

4. Detailed design

4.1 (CSC name and project-unique identifier)
(Additional Security Requirements Apply)

4.1.1 (CSU name and project-unique identifier)
(Additional Security Requirements Apply)

4.1.1.1 (CSU name) Design specification/constraints
(Additional Security Requirements Apply)

4.1.1.2 (CSU name) Design
(Additional Security Requirements Apply)

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 8)

Software Design Document (continued)

4.1.1.2.a Input/output data elements

4.1.1.2.b Local data elements

4.1.1.2.c Interrupts and signals

4.1.1.2.d Algorithms

4.1.1.2.e Error handling

4.1.1.2.f Data conversion

4.1.1.2.g Use of other elements

4.1.1.2.g.1 (Other CSUs)

4.1.1.2.g.2 (Shared data)

4.1.1.2.g.3 (Input/output buffers)

4.1.1.2.h Logic flow

4.1.1.2.i Data structures

4.1.1.2.j Local data files or database

4.1.1.2.k Limitations

5. CSCI data

(Additional Security Requirements Apply)

5.a (CSCI-internal data elements)

5.a.1 (Data element name)

5.a.2 (Data element description)

5.a.3 (Units)

5.a.4 (Limit/range)

5.a.5 (Accuracy)

5.a.6 (Precision)

5.a.7 (Frequency of calculation or refresh)

5.a.8 (Legality checks)

5.a.9 (Data type)

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 9)

Software Design Document (continued)

5.a.10 (Data representation/format)

5.a.11 (CSUs that set the data element)

5.a.12 (CSUs that use the data element)

5.a.13 (Source)

5.b (CSCI-external data elements)

5.b.1 (Data element name)

5.b.2 (Interface involved)

5.b.3 (IDD that describes the interface)

6. CSCI data files
(Additional Security Requirements Apply)

6.1 Data file to CSC/CSU cross reference

6.2 (Data file name and project-unique identifier)

7. Requirements traceability

8. Notes

(Appendixes)
(Additional Security Requirements Apply)

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 10)

Software Development Plan (SDP)

1. Scope

1.1 Identification

1.2 System overview

- 1.3 Document overview
- 1.4 Relationship to other plans
(Additional Security Requirements Apply)
- 2. Referenced documents
- 3. Software development management
 - 3.1 Project organization and resources
 - 3.1.1 Contractor facilities
 - 3.1.2 Gov't furnished equipment, software, services
 - 3.1.3 Organizational structure
 - 3.1.4 Personnel
 - 3.2 Schedule and milestones
 - 3.2.1 Activities
 - 3.2.1.a (Activity initiation)
 - 3.2.1.b (Availability of documentation)
 - 3.2.1.c (Activity completion)
 - 3.2.1.d (Areas of high risk)
 - 3.2.2 Activity network
 - 3.2.3 Source Identification
 - 3.3 Risk management
 - 3.3.a (Areas of risk)
 - 3.3.b (Constituent risk factors)

3.3.c (Risk monitoring and reduction)

3.3.d (Contingency procedures)

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 11)

Software Development Plan (continued)

3.4 Security

(Additional Security Requirements Apply)

3.5 Interface with associate contractors

3.6 Interface with software IV&V agent(s)

3.7 Subcontractor management

3.8 Formal reviews

3.9 Software development library

3.10 Corrective action process

3.11 Problem/change report

3.11.a System or project name

3.11.b Originator

3.11.c Problem number

3.11.d Problem name

3.11.e Software element or document affected

3.11.f Origination date

3.11.g Category and priority

3.11.h Description of problem

3.11.i Analyst

3.11.j Date assigned

3.11.k Date complete

3.11.l Analysis time

3.11.m Recommended solution

3.11.n Impacts

3.11.o Problem status

3.11.p Approval of solution

3.11.q Follow-up action

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 12)

Software Development Plan (continued)

3.11.r Corrector

3.11.s Correction date

3.11.t Version number

3.11.u Correction time

3.11.v Implementation solution

4. Software engineering

4.1 Organization and resources - s/w engineering

4.1.1 Organizational structure - software engineering

4.1.2 Personnel - software engineering

4.1.3 Software engineering environment

4.1.3.1 Software items

4.1.3.2 Hardware and firmware items

4.1.3.3 Proprietary nature and Government rights

4.1.3.4 Installation, control, and maintenance

4.2 Software standards and procedures

4.2.1 S/W development techniques and methodologies
(Additional Security Requirements Apply)

4.2.1.a (Software requirements analysis)

4.2.1.b (Preliminary design)

4.2.1.c (Detailed design)

4.2.1.d (Coding and CSU testing)

4.2.1.e (CSC integration and testing)

4.2.1.f (CSCI testing)

4.2.2 Software development files

4.2.3 Design standards
(Additional Security Requirements Apply)

4.2.4 Coding standards

Software Development Plan (continued)

- 4.3 Non-developmental software
- 5. Formal qualification testing
 - 5.1 Organization and resources - FQT
 - 5.1.1 Organizational structure - FQT
 - 5.1.2 Personnel - formal qualification testing
 - 5.2 Test approach/philosophy
 - 5.3 Test planning assumptions and constraints
- 6. Software product evaluations
 - 6.1 Organization and resources - s/w product evals
 - 6.1.1 Organizational structure - s/w product evals
 - 6.1.2 Personnel - software product evaluations
(Additional Security Requirements Apply)
 - 6.2 S/W product evaluations procedures and tools
 - 6.2.1 Procedures
 - 6.2.2 Tools
 - 6.3 Subcontractor products
 - 6.4 Software product evaluation records
 - 6.5 Activity-dependent product evaluations
 - 6.5.1 Software products evaluation - (activity name)

7. Software configuration management

7.1 Organization and resources - config. management

7.1.1 Organizational structure - config. management

7.1.2 Personnel - configuration management

7.2 Configuration identification

7.2.1 Developmental configuration identification

7.2.2 Identification methods

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 14)

Software Development Plan (continued)

7.3 Configuration control

7.3.1 Flow of configuration control

7.3.2 Reporting documentation

7.3.2.1 (Report name)

7.3.3 Review procedures

7.3.3.1 (Review board name) procedures

7.3.4 Storage, handling, delivery of project media

7.3.5 Additional control

7.4 Configuration status accounting

7.5 Configuration audits

7.6 Preparation for specification authentication

7.6.a (Submitting specifications)

7.6.b (Ensuring incorporation of approved changes)

7.6.c (Updating configuration status reports)

7.7 Configuration management major milestones

8. Other software development functions

(Additional Security Requirements Apply)

8.1 (Function name)

8.1.1 Organizational structure - (function name)

8.1.2 Personnel - (function name)

8.1.3 Other resources - (function name)

8.1.4 Methods and procedures - (function name)

9. Notes

(Appendixes)

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 15)

Software Requirements Specification (SRS)

1. Scope

1.1 Identification

1.2 CSCI overview

1.3 Document overview

2. Applicable documents

2.1 Government documents

2.2 Non-Government documents

3. Engineering requirements

(Delete reference to PIDS and CIDS.)

3.1 CSCI external interface requirements

(Additional Security Requirements Apply)

3.2 CSCI capability requirements

3.2.1 (Capability name and project-unique identifier)

3.3 CSCI internal interfaces

3.4 CSCI data element requirements

3.4.a (CSCI-internal data elements)

3.4.a.1 (Data element identifier)

3.4.a.2 (Data element description)

3.4.a.3 (Units)

3.4.a.4 (Limit/range)

3.4.a.5 (Accuracy)

3.4.a.6 (Precision)

3.4.a.7 (Internal interfaces)

3.4.b (CSCI-external data elements)

3.4.b.1 (Data element identifier)

3.4.b.2 (Interface identifier)

3.4.b.3 (Source or destination capability)

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 16)

Software Requirements Specification (continued)

3.4.b.4 (Reference to applicable IRS)

3.5 Adaptation requirements

3.5.1 Installation-dependent data

3.5.2 Operational parameters

3.6 Sizing and timing requirements

3.7 Safety requirements

3.8 Security requirements
(Additional Security Requirements Apply)

3.9 Design constraints
(Additional Security Requirements Apply)

3.10 Software quality factors
(Additional Security Requirements Apply)

3.11 Human performance/human engineering requirements

3.11.a (Human capabilities and limitations)

3.11.b (Foreseeable human errors)

3.11.c (Implications for total system environment)

3.12 Requirements traceability
(Delete references to PIDS and CIDS. Additional Security)

4. Qualification requirements

4.1 Qualification methods

(Additional Security Requirements Apply)

4.2 Special qualification requirements

4.2.a (Test identifier)

4.2.b (Capability requirements addressed)

4.2.c (Description of the test)

4.2.d (Test level)

5. Preparation for delivery

6. Notes

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 17)

Software Requirements Specification (continued)

(Appendixes)

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 18)

System/Segment Design Document (SSDD)

1. Scope

1.1 Identification

- 1.2 System overview
 - (Additional Security Requirements Apply)
- 1.3 Document overview
- 2. Referenced documents
- 3. Operational concepts
 - 3.1 Mission
 - 3.1.1 User needs
 - 3.1.2 Primary mission(s)
 - 3.1.3 Secondary mission(s)
 - 3.2 Operational environment
 - 3.3 Support environment
 - 3.3.1 Support concept
 - 3.3.1.a (Multipurpose or automated test equipment)
 - 3.3.1.b (Repair vs replacement criteria)
 - 3.3.1.c (Levels of maintenance)
 - 3.3.1.d (Maintenance and repair cycles)
 - 3.3.1.e (Government and contractor support)
 - 3.3.1.f (Accessibility)
 - 3.3.1.g (Other support concept topics)
 - 3.3.2 Support facilities
 - 3.3.3 Supply
 - 3.3.3.a (Introduction of new items)

3.3.3.b (Re-supply methods)

3.3.3.c (Distribution and location of system stocks)

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 19)

System/Segment Design Document (continued)

3.3.4 Government agencies

3.4 System architecture
(Additional Security Requirements Apply)

3.5 Operational scenarios

4. System design

4.1 HWCI identification

4.1.1 (HWCI name and project-unique identifier)
(Additional Security Requirements Apply)

4.2 CSCI identification

4.2.1 (CSCI name and project-unique identifier)
(Additional Security Requirements Apply)

4.3 Manual operations identification

4.3.1 (Manual operation name and identifier)

4.4 Internal interfaces

4.4.1 (HWCI-to-HWCI interface name and identifier)

4.4.2 (HWCI-to-CSCI interface name and identifier)

4.4.3 (CSCI-to-CSCI interface name and identifier)

5. Processing resources

5.1 Processing resource name and identifier

5.1.a Memory size

5.1.b Word size

5.1.c Processing speed

5.1.d Character set standard

5.1.e Instruction set architecture

5.1.f Interrupt capabilities

5.1.g Direct Memory Access (DMA)

5.1.h Channel requirements

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 20)

System/Segment Design Document (continued)

5.1.i Auxiliary storage

5.1.j Growth capabilities

5.1.k Diagnostic capabilities

5.1.l Additional computer hardware capabilities

5.1.m Processing resource allocation

6. Quality factor compliance

7. Requirements traceability

8. Notes

(Appendixes)

DOCUMENT OUTLINE REPORT for SDE, 5/27/92, 22:38 (page 21)

Software User's Manual (SUM)

1. Scope

1.1 Identification

1.2 System overview

1.3 Document overview

2. Referenced documents

3. Execution procedures
(Additional Security Requirements Apply)

3.a Initialization

3.b User inputs

3.c System inputs

3.d Termination

3.e Restart

3.f Outputs

4. Error messages

5. Notes

(Appendixes)

6 Conclusions

This report has described the results of the Integrated Trusted System Development Environment (ITSDE) project. The project developed Integrated Data Item Descriptions (DID's) for use with the Integrated Development Process defined in [BENZEL]. In this report we have presented our results in three forms: Tailoring Guidance, Integrated DID's, and Document Outline Reports. We believe that presenting our results in these varied fashions will increase their usefulness and allow the IDP and the corresponding DID's to be widely applicable.

Data Item Descriptions (DID's) and the resulting software Development documents are not sufficient alone. Just as important as determining *which* documents to deliver is deciding *when* documents should be delivered and how they should be reviewed. DoD-STD-2167A prescribes when documents should be developed and DoD-STD-2168 prescribes the requirements for the conduct of the technical reviews and audits of the documents. Both of these standards along with the IDP should be re-examined in order to determine whether changes should be made to address the development and review of the documents resulting from the integrated and newly developed DID's.

The Harmonization Working Group (HWG) of the Department of Defense Software Action Plan (SWAP) and the Joint Logistics Commanders Joint Policy Coordinating Group on Computer Resource Management (JLC-JPCG-CRM) is developing MIL-STD-SDD which is a new Software Development and Documentation standard. The Working Group has decided to address security requirements in the new standard and is very interested in the Integrated DID's described in this report. Thus, in addition to addressing these issues in the context of the current standards we will need to examine lifecycle issues as the new SDD standard is developed.

References

- [BENZEL] Benzel, T.C.V., "Developing Trusted Systems Using DoD-STD-2167A" Proceedings of the Fifth Annual Computer Security Applications Conference, Tucson, Arizona, December 1989.
- [BODEAU] Bodeau, D.J., "TCSEC Specification and Verification Documentation Applicability: Interim Report", WP-27545, The MITRE Corporation, Bedford, MA, September 1987.
- [DOD] "Department of Defense Trusted Computer System Evaluation Criteria." DOD 5200.28-STD, December 1985.
- [FREEMAN] Personal Communication (email) James W. Freeman, October 1991.
- [JLC] "Proceedings JLC-CRM 4th Biennial Software Workshop, Orlando II", 23 March 1987.
- [KELLY] Security Guide for Security-Relevant CDRL's and DID's. DRAFT. AFCSC/SRXP. San Antonio Texas, 1988.
- [LOGICON] TAILOR 2167A, Logicon, San Diego, CA 1989.
- [MINUTES] "Minutes of the Trusted Software Development Workshop 21 October 1988". Pfleeger, C.P., T.C.V. Benzel, L.D. Martin. TIS-R-197, Trusted Information Systems Inc., Glenwood, MD, 14 December 1988.
- [490A] MIL-STD-490A, Military Standard: Specification Practices. Department of Defense, 4 June 1985.
- [2167A] DOD-STD-2167A, Military Standard: Defense System Software Development, 29 February 1988.
- [2168] DOD-STD-2168, Military Standard: Defense System Software Quality Program, 29 April 1988.

MISSION
OF
ROME LABORATORY

Rome Laboratory plans and executes an interdisciplinary program in research, development, test, and technology transition in support of Air Force Command, Control, Communications and Intelligence (C3I) activities for all Air Force platforms. It also executes selected acquisition programs in several areas of expertise. Technical and engineering support within areas of competence is provided to ESC Program Offices (POs) and other ESC elements to perform effective acquisition of C3I systems. In addition, Rome Laboratory's technology supports other AFMC Product Divisions, the Air Force user community, and other DOD and non-DOD agencies. Rome Laboratory maintains technical competence and research programs in areas including, but not limited to, communications, command and control, battle management, intelligence information processing, computational sciences and software producibility, wide area surveillance/sensors, signal processing, solid state sciences, photonics, electromagnetic technology, superconductivity, and electronic reliability/maintainability and testability.